UNIVERSIDAD DE LA RIOJA

TRABAJO FIN DE ESTUDIOS

Título

Introducción al Álgebra Homológica

Autor/es

HÉCTOR GUTIÉRREZ MUÑOZ

Director/es

JESÚS ANTONIO LALIENA CLEMENTE

Facultad

Facultad de Ciencia y Tecnología

Titulación

Grado en Matemáticas

Departamento

MATEMÁTICAS Y COMPUTACIÓN

Curso académico

2016-17

publicaciones.unirioja.es
E-mail: publicaciones@unirioja.es

UNIVERSIDAD DE LA RIOJA

Facultad de Ciencia y Tecnología

TRABAJO FIN DE GRADO

Grado en Matemáticas

Introducción al Álgebra Homológica

Alumno:

Héctor Gutiérrez Muñoz

Tutores:

Jesús Laliena Clemente

Logroño, junio de 2017

Resumen

En este trabajo se presenta una introducción al álgebra homológica. Para ello, se comienza introduciendo los aspectos más importantes de la teoría de módulos y a continuación se explican ciertas nociones sobre categorías, sentando así las bases del lenguaje con el que más adelante se desarrollará la homología. Tras introducir estas nociones previas y profundizar en los módulos proyectivos e inyectivos, se desarrollan las herramientas más básicas del álgebra homológica, culminando con la introducción de los funtores derivados. Finalmente, se comentan brevemente dos de las aplicaciones más importantes de la homología: su aportación al problema de la extensión de grupos y sus usos dentro del campo de la topología algebraica.

Abstract

In this paper we introduce the theory of homological algebra. In first place, we will begin studying the most relevant aspects of the theory of modules, following that by some insights in category theory, thus laying down the foundations on which the homological algebra will be based. After studying these preliminary notions and focusing on projective and injective modules, the most important tools in the theory of homological algebra are introduced, concluding with the definition of a derived functor. Finally, we briefly comment on two of the most important applications of the homology theory, presenting in first place the problem of group extension and concluding with some of the uses of homology in the field of algebraic topology.

Índice

1. Introducción

La homología es un área de las matemáticas relativamente reciente. Una exhaustiva historia de este campo se puede encontrar en [2]. Resumiendo, se puede decir que la homología nació cuando H. Poincaré (matemático francés, 1854-1912) hizo por primera vez referencia a este concepto al identificar espacios topológicos con objetos algo complejos y no simplemente numéricos en su *Analysis Situs* (1895). Es más, podríamos definir a muy grandes rasgos la homología como la asociación de objetos matemáticos de muy dispar naturaleza. Desde su nacimiento a finales del siglo XIX, la homología comenzó un largo proceso de gestación hasta el comienzo de la Segunda Guerra Mundial, cuando los conceptos de homología y cohomología en un espacio topológico quedaron bien definidos.

Esta primera etapa de la homología que surgió a raíz de la gran intuición de Poincaré duró alrededor de medio siglo y a ella contribuyeron matemáticos de distintas escuelas como el austriaco W. Mayer (1887-1948), el alemán H. Hopf (1894-1971), la alemana E. Noether (1882-1935) o más tarde el ruso P. Alexandroff (1896-1982). A partir de 1940, a este trabajo le siguió siguió el del matemático francés H. Cartan (1904-2008) y el polaco S. Eilenberg (1913-1998). Estos dos autores, al introducir el rigor que con el paso de los años aumentaba cada vez más en las matemáticas y unificar todos los resultados existentes, se dieron cuenta de que la homología no solo tenía sentido encuadrada dentro de la topología, sino que se podía extender a un contexto algebraico mucho más general. Su trabajo culminó en 1956 con la publicación conjunta de [1], el libro que popularizó la homología en un contexto algebraico, cuando ya la teoría estaba mucho más madura que un par de décadas atrás.

En el prefacio a [1], Cartan y Eilenberg motivaron el álgebra homológica como una teoría que unificaba todos los resultados de homología y cohomología desarrollados para diversas estructuras como grupos, álgebras de Lie y álgebras asociativas, transcendiendo así el alcance inicial del estudio de los grupos de homología para espacios topológicos y además añadiendo resultados adicionales que serían imposibles de hallar sin esta teoría. En este importantísimo libro, la mayoría de conceptos homológicos se presentan de forma similar a la actual, similar también a la forma en la que se recogen en este trabajo.

Las herramientas homológicas, que en un principio eran miradas con cierto escepticismo por una parte de la comunidad matemática, fueron resultando útiles para resolver problemas en áreas muy distintas de la ciencia. Incluso aspectos homológicos que parecían muy oscuros o sin aplicaciones se mostraron más tarde importantes en sitios insospechados. De esta forma, el álgebra homológica siguió desarrollándose en gran medida al menos durante un par de décadas más, con el trabajo de matemáticos como A. Grothendieck (1928-2014).

En esta memoria se desarrollarán las herramientas homológicas más importantes y que representan la base fundamental del álgebra homológica, comenzando por la definición de los complejos y acabando con la construcción de los funtores derivados, atendiendo en particular a los funtores Ext. Para poder hacer este desarrollo, se necesitará previamente introducir la teoría de categorías (de donde sale el concepto de funtor, por ejemplo) y dar unas nociones de teoría de módulos. Para esta tarea no se siguió [1], libro que ya queda algo desfasado, sino que se recurrió a [4, cap. 1, 3 y 6], uno de los libros generales de álgebra más usados entre los matemáticos. Además, y sobre todo para la parte de módulos, nos apoyamos también en [3, cap. 4].

Como punto final del trabajo, para así cerrarlo con algo más ilustrativo y además demostrar la utilidad de la teoría desarrollada, se presentarán dos de las aplicaciones más importantes del álgebra homológica. En primer lugar se hablará del problema de la extensión de grupos y para cerrar, se darán ciertas pinceladas sobre las aplicaciones de la homología a la topología algebraica (para este último apartado se ha consultado también [5]).

Para finalizar esta introducción, me gustaría aclarar que la filosofía al escribir este trabajo ha sido la de obtener algo autocontenido y orientado a desarrollar la teoría necesaria para desarrollar las aplicaciones mencionadas. Esta consideración unida al deseo de no extenderme demasiado en la redacción, ha llevado a que en ciertas secciones se haya preferido introducir resultados o conceptos de menor importancia general pero que más adelante serían necesarios antes que otros temas que pudieran tener más interés de forma general.

2. Módulos

En esta primera sección haremos una pequeña incursión dentro de la teoría de módulos. Como muchas otras nociones en matemáticas, la estructura de módulo nació como una generalización de otra ya existente, en este caso de los espacios vectoriales.

A principios del siglo XX, el álgebra lineal solamente se había desarrollado como el estudio de espacios vectoriales sobre los reales o los complejos. Sin embargo, pronto se alcanzó el consenso de que esta restricción no tenía sentido, ya que la mayoría de resultados se basaban solamente en la solución de ecuaciones lineales válidas para cualquier cuerpo. De esta forma, pronto el álgebra lineal se generalizó al estudio de espacios vectoriales sobre cualquier cuerpo, tal y como ahora lo conocemos.

Sin embargo, a partir de esta primera generalización surgió una segunda también bastante natural: el estudio de unos "espacios vectoriales" sobre un anillo cualquiera que no tuviera por qué tener estructura de cuerpo. Básicamente, esta generalización constituye un módulo.

En este trabajo, y por cuestiones de extensión, solo presentaremos unos conceptos muy básicos de la teoría de módulos, con vistas simplemente a introducir lo necesario para desarrollar la teoría homológica más adelante. Comenzaremos de esta forma con la definición de módulo y sus propiedades más básicas. Después, pasaremos a las sumas directas de módulos y al concepto de módulo libre, parte fundamental de la sección. Por último, introduciremos unos tipos particulares de módulos: proyectivos e inyectivos, que estudiaremos con más profundidad en secciones posteriores. Esto se debe a que resultan muy interesantes dentro del álgebra homológica, pero tiene mucho más sentido tratar con ellos una vez hayamos introducido el lenguaje categórico de la sección 3.

Por desgracia, no se podrá dar más profundidad a esta sección, con lo que partes muy importantes de la teoría de módulos como sus aplicaciones al álgebra lineal (permitiendo probar muy fácilmente resultados conocidos sobre espacios vectoriales, generalizándolos y desarrollándolos más), a la teoría de grupos (permitiendo llegar a la clasificación de grupos abelianos) o la noción de producto tensorial (motivada por la necesidad de "multiplicar" elementos de dos módulos distintos como puede ser el caso de valores propios complejos y vectores reales) quedarán fuera del trabajo, entre muchos otros aspectos.

2.1. Definiciones y propiedades básicas

Definición 2.1 (Módulo sobre un anillo R)**.** *Sea R un anillo. Un grupo abeliano M se dice un R-módulo (a izquierda) si tiene definida una operación $(r, x) \mapsto rx \in M$ de forma que*

(i) $r(x + y) = rx + ry$,

(ii) $(r + s)x = rx + sx$,

(iii) $(rs)x = r(sx)$

se cumplen para todo $r, s \in R$, $x, y \in M$ (notemos que M se suele escribir como un grupo aditivo).

Las palabras "a izquierda" pueden omitirse, pero a veces son necesarias para distinguir estos módulos de los R-módulos a derecha, los cuales se definen de forma similar pero invirtiendo el orden de los elementos r y x en la multiplicación. Además, de las tres condiciones anteriores se sigue inmediatamente que en los R-módulos a izquierda $r \cdot 0 = 0 \cdot x = 0$ y $(-r)x = x(-r) = -rx$ bajo los supuestos de la definición (y análogo para los módulos a derecha).

La definición de módulo no es nada arbitraria: tomando $R = \mathbb{F}$, un cuerpo, y $M = V$, un espacio vectorial cualquiera sobre $\mathbb{F}$, las propiedades de módulo tienen el sentido natural del producto por un escalar. Esto se debe a que como hemos comentado antes, la teoría de módulos es en cierto sentido un intento de generalizar el álgebra lineal permitiendo un conjunto más general de escalares. Pero no solo podemos obtener los espacios vectoriales como caso particular de los módulos. Si se toma $R = \mathbb{Z}$ y M un grupo abeliano cualquiera, el producto rx ya tiene un significado definido en teoría de grupos para todo $r \in \mathbb{Z}$, $x \in M$ y cumple las tres propiedades de la definición de módulo. De esta forma, la teoría de grupos abelianos también se puede considerar incluida en la de módulos.

A partir de la definición de módulo, se pueden definir de forma totalmente natural otros conceptos relacionados y análogos a los de otras estructuras:

Definición 2.2 (Más definiciones sobre módulos)**.** *Para cualquier R-módulo M, se define lo siguiente:*

(i) En el caso de que el anillo R sea unitario, M se dirá unitario si $1 \cdot x = x$ para todo $x \in M$.

(ii) Un subgrupo N de M se llamará submódulo de M si $rx \in N$ para todo $r \in R$, $x \in N$.

(iii) Si N es un submódulo de M, el grupo cociente M/N es también un R-módulo, llamado módulo cociente, si definimos $r(x + N) = rx + N$ para todo $r \in R$, $x \in M$.

Tras el introducir el concepto de submódulo se puede dar la siguiente proposición:

Proposición 2.3. *Si M es un R-módulo y $\{M_\alpha\}$ es una familia de submódulos de M no vacía, entonces $\bigcap_\alpha M_\alpha$ es también un submódulo de M.*

La prueba se omite por su sencillez. Notemos además que en el enunciado se ha omitido la condición de que α pertenezca a un cierto conjunto de índices. Durante todo el trabajo, cuando no haya lugar a duda sobre cuál es este conjunto de índices o cuando pueda ser cualquiera también se omitirá. Esto se hace para más adelante no sobrecargar ni los enunciados ni las pruebas cuando sean más complicados. De todas formas, en ningún caso dejaremos lugar a dudas o a que surja cierta ambigüedad.

Para nosotros, lo más interesante de la proposición anterior es que si M es un R-módulo y $S \subseteq M$ es un subconjunto cualquiera, entonces existe un único submódulo mínimo de M que contiene a S. Lo denotaremos como $R\langle S\rangle$ y lo llamaremos *submódulo de M generado por S* (o *finitamente generado* si S es finito). Además, si $M = R\langle a\rangle$ para algún elemento $a \in M$, diremos que M es *cíclico* sobre R.

Respecto a las aplicaciones entre módulos, podemos definir los siguientes conceptos de forma similar a lo ya conocido para otras estructuras:

Definición 2.4 (Homomorfismo de módulos)**.** *Si M y N son dos R-módulos, un homomorfismo (o R-homomorfismo) de M a N es un homomorfismo de grupos $f : M \to N$ tal que $f(rx) = rf(x)$ para todo $r \in R$, $x \in M$. Denotaremos el conjunto de homomorfismos entre estos dos módulos como* $\hom_R(M, N)$*, pudiendo omitir la R si no hay lugar a duda.*

A partir de esta definición, los conceptos de *isomorfismo*, *automorfismo*, *imagen* (submódulo de N), *núcleo* (submódulo de M)... se definen como de costumbre. Incluso los tres teoremas básicos de isomorfía ya conocidos de anillos o grupos se pueden establecer análogamente para módulos.

No desarrollaremos más las nociones anteriores por no hacer demasiado larga esta sección. Sin embargo, un último concepto nuevo y que será de un gran interés más adelante es el siguiente:

Definición 2.5 (Sucesión exacta de módulos)**.** *Una sucesión de módulos $\{M_i\}$ conectados por homomorfismos $\{f_i\}$ de la siguiente forma*

$$\cdots \longrightarrow M_{i-2} \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \cdots$$

se dirá exacta si para todo i se cumple que $\operatorname{im} f_{i-1} = \ker f_i$.

Como caso particular, nos interesarán las *sucesiones exactas cortas*, es decir, sucesiones de la forma $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ en las que, debido a la exactitud, f es inyectiva, g sobreyectiva y se cumple que $\operatorname{im} f = \ker g$.

2.2. Sumas directas

La construcción y definición de un producto directo para una familia no vacía $\{M_\alpha\}$ de R-módulos es totalmente análoga a la del producto directo de grupos, por lo que no se repetirá aquí. Simplemente recordaremos que este producto de módulos lo denotaremos como $\prod M_\alpha$ o $M_1 \times M_2 \times \cdots \times M_n$ si la familia es finita. Sin embargo, sí presentaremos a continuación la noción de *suma directa* y ahondaremos en ella por la relevancia que tiene dentro de la teoría de módulos.

Definición 2.6 (Suma directa de módulos)**.** *Sea $\{M_\alpha\}_{\alpha\in A}$ una familia no vacía de R-módulos. Una suma directa de la familia anterior es otro R-módulo M junto con una familia de homomorfismos $i_\alpha : M_\alpha \to M$, $\alpha \in A$ de forma que para todo R-módulo N y homomorfismos $f_\alpha : M_\alpha \to N$, $\alpha \in A$, existe un único $f \in \hom_R(M, N)$ tal que $fi_\alpha = f_\alpha$ para todo $\alpha \in A$.*

Muchas veces, a una suma directa (M, i_α) se la denotará simplemente como M por brevedad, y para referirnos a la suma directa de una familia de R-módulos como la anterior se usará la notación $\oplus M_\alpha$, o $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ si la familia es finita.

Veamos de forma constructiva que la definición dada es válida, es decir, que efectivamente esta suma directa existe y además es única (salvo isomorfismo) para cualquier familia de módulos:

Proposición 2.7 (Existencia y unicidad de la suma directa)**.** *Cualquier familia no vacía $\{M_\alpha\}_{\alpha\in A}$ de R-módulos tiene una suma directa. Además, dicha suma directa es única salvo isomorfismo.*

Demostración. Sea M el submódulo de $\prod M_\alpha$ que contiene a los elementos m del producto tales que sus proyecciones m_α son nulas para todos los $\alpha \in A$ salvo, como mucho, un conjunto finito. Veamos que este M constituye una suma directa para la familia $\{M_\alpha\}$. Definimos para ello $i_\alpha : M_\alpha \to M$ para cada α de forma que $i_\alpha(x) = m$ si y solo si la α-ésima proyección de m es igual a x y el resto son 0 (es obvio que $i_\alpha \in \hom(M_\alpha, M)$, está correctamente definida). Ahora, para cualquier R-módulo N junto con una familia de homomorfismos $f_\alpha : M_\alpha \to N$ definimos $f : M \to N$ de forma que $f(m) = \Sigma\{f_\alpha(m_\alpha) : \alpha \in A\}$ (bien definida ya que solo hay un número finito de sumandos no nulos). De esto se sigue que $f \in \hom(M, N)$, $fi_\alpha = f_\alpha$ para todo α y es inmediato ver que f está unívocamente determinada.

Tras demostrar la existencia de una suma directa $(M, \{i_\alpha\})$, supongamos que la pareja $(M', \{i'_\alpha\})$ es otra suma directa de la familia $\{M_\alpha\}$. Entonces, tomando la pareja $(N, \{f_\alpha\})$ de la definición como $(M', \{i'_\alpha\})$ en el primer caso y $(M, \{i_\alpha\})$ en el segundo, tendremos que existen unas f, f' tales que $fi_\alpha = i'_\alpha$ y $f'i'_\alpha = i_\alpha$. De esta forma, $i_\alpha = f'i'_\alpha = f'fi_\alpha$, con lo que $f'f = 1_M$ (la aplicación identidad en M) y procediendo de forma inversa, $ff' = 1_{M'}$. De esta forma f y g son una pareja de isomorfismos inversos entre M y M' y la suma directa es por tanto única salvo isomorfismo. □

Aunque no se pruebe explícitamente aquí, no es difícil concluir además que cada uno de los i_α de la definición de suma directa es un monomorfismo. Esto lleva en parte a que si $M = \oplus M_\alpha$, cada elemento $x \in M$ se podrá expresar como $x = x_1 + x_2 + \cdots + x_k$ para algún k con los $x_i \in M_{\alpha_i}$.

2.3. Módulos libres

Tras haber definido la suma directa de módulos, podemos comenzar a hablar de algo que parece natural como es la existencia de bases para módulos, siendo estos una generalización de los espacios vectoriales. Sin embargo, nos encontramos con que un gran número de módulos no poseen nada parecido a una base, siendo los conocidos como *módulos libres* los únicos donde se puede definir algo similar al concepto de base ya conocido.

Definición 2.8 (Módulo libre)**.** *Sea R un anillo unitario y B un conjunto cualquiera. Un R-módulo libre con base B es un R-módulo unitario F junto con una función $\phi : B \to F$ de forma que dados cualquier R-módulo unitario M y cualquier función $\theta : B \to M$, existe un único homomorfismo $f \in \hom(F, M)$ tal que $f\phi = \theta$.*

Como hemos hecho antes, comprobaremos rápidamente que efectivamente esta definición es correcta (es decir, que los módulos libres efectivamente existen y son únicos salvo isomorfismo).

Partiendo de un conjunto B no vacío, consideremos al anillo R como un R-módulo (es trivial ver que todo anillo es un módulo sobre sí mismo) y tomemos $F = \oplus_{\alpha\in B} R_\alpha$ con $R_\alpha = R$ para todo $\alpha \in B$ (es decir, construimos F como la suma directa de $|B|$ copias del R-módulo R). Además, para cada $\beta \in B$, definimos $\phi(\beta) = m \in F$ con m el elemento de la suma directa F para el cual $m_\beta = 1 \in R$ y $m_\alpha = 0$ para el resto de $\alpha \in B$, $\alpha \neq \beta$. Terminar de ver que F junto con ϕ forman un R-módulo libre con base B es trivial, así como ver que esta suma directa es isomorfa a cualquier otra que se pueda definir.

A partir de la construcción anterior de $\phi : B \to F$, podemos identificar cada elemento $\beta \in B$ con su imagen $\phi(\beta)$, asumiendo así que $B \subseteq F$ y permitiendo expresar los elementos de F como combinación lineal de los de B, como es normal en otras estructuras.

Además, de esta forma se puede hablar de que un subconjunto B' de M es R-*linealmente independiente* si dados $b_1, ..., b_k \in B'$ y $r_1, ..., r_k \in R$ con $\sum r_j b_j = 0$ podemos concluir que todos los $r_j = 0$. Es obvio por la construcción que esto se cumple para $B' = B$ en un R-módulo M con base B. Además, si el conjunto anterior B' cumple que $M = R\langle B'\rangle$, diremos que B' es una base de M (algo que también se cumple para $B' = B$ en un R-módulo con base B). Es más, podemos asegurar que un R-módulo unitario es libre si y solo si tiene una base como acabamos de construir.

Como se puede ver, en el caso de los módulos la definición de base no es tan natural como a priori podía parecer y presenta ciertas particularidades que no ocurren en otras estructuras. Por ejemplo, dos bases de un R-módulo F no tienen por qué tener la misma cardinalidad. Para que eso ocurra, el anillo unitario R debe tener un ideal I tal que R/I sea un anillo de división. En este caso, la cardinalidad de cualquier base se dirá *rango* del módulo. Un caso particular que tiene bastante interés se tiene al tomar $R = \mathbb{Z}$. Los enteros cumplen la condición anterior (ya que forman un anillo conmutativo y esto implica que la condición anterior se cumple). De esta forma, si repetimos lo anterior para $\mathbb{Z}$-módulos (es decir, grupos abelianos como comentamos al principio de la sección), podremos ver que un *grupo abeliano libre* es una suma directa de algún número de copias de $\mathbb{Z}$ como grupo aditivo en donde además se puede hablar de rango.

2.4. Introducción a los módulos proyectivos e inyectivos

Veremos más adelante que una generalización del concepto de módulo libre que resulta mucho más interesante y natural es la de *módulo proyectivo*. Sin embargo, para definirlo y manipularlo de una forma más sencilla se necesita haber introducido el lenguaje categórico. Es por esto que en esta sección solamente se introduce el concepto de proyectividad y no será hasta el apartado 4.0, justo antes de comenzar la parte de homología, en donde se desarrolle más a fondo. Además, esto se debe que los módulos proyectivos tienen una gran relevancia en el álgebra homológica.

Definición 2.9 (Módulo proyectivo)**.** *Sea R un anillo unitario. Un R-módulo P se dice proyectivo si dada una sucesión exacta $M \xrightarrow{g} N \to 0$ y un homomorfismo $f : P \to N$, existe otro homomorfismo $h : P \to M$ tal que $f = gh$.*

Los módulos inyectivos aparecen a partir de esta definición de los proyectivos mediante una transformación que introduciremos al hablar de categorías. Estos módulos también tienen cierta importancia dentro del álgebra homológica. Sin embargo, para ellos ni siquiera se dará la definición aquí sino que se esperará al apartado 4.0.

3. Categorías

En esta sección se presentan las nociones más importantes dentro de la teoría de categorías. Su interés reside en que permite unificar un buen número de aspectos relativos a múltiples estructuras matemáticas. Si bien esta teoría no proporciona una estructura concreta, sí que da un lenguaje y un buen número de herramientas que han tenido una gran relevancia en el desarrollo más moderno del álgebra, la geometría, la topología y otras áreas de la ciencia relacionadas con ellas.

El concepto central de la sección es el de categoría, la cual está compuesta por objetos y morfismos. La noción de categoría generaliza la noción de una una estructura algebraica, topológica o geométrica cualquiera, ya que una estructura tiene como nociones asociadas principales unos ciertos objetos (conjuntos con operaciones o algunas propiedades) y unas ciertas aplicaciones entre ellos (homomorfismos para los grupos, aplicaciones continuas para los espacios topológicos...). De esta forma, abstrayendo lo que define una estructura cualquiera, la teoría de categorías aspira a dar resultados generales para un gran número de estructuras distintas y a a ser capaz de trasladar aspectos conocidos de unas estructuras a otras.

Después de dar la definición de categoría y unos primeros ejemplos, pasaremos a estudiar el concepto asociado de funtor. Esta es la herramienta categórica que permite el "movimiento" entre diversas estructuras, trasladando conceptos y resultados de una a otra. Finalizaremos la sección estudiando unos ejemplos bastante concretos de funtores y categorías que cobrarán bastante relevancia en siguiente sección sobre homología.

Nuevamente, por no alargar demasiado esta sección, hay temas de gran importancia dentro de la teoría de categorías que apenas se tocarán. Desde las transformaciones naturales y las equivalencias de categorías, que en ciertos ámbitos presentan una de las motivaciones más importantes para estudiar esta teoría, a la definición de un universal, un buen número de aspectos muy importantes se han tenido que dejar fuera del trabajo.

3.1. Definición y ejemplos

Formalmente, el concepto de *categoría* se define como sigue:

Definición 3.1 (Categoría)**.** *Una categoría* $\mathbf{C}$ *consiste en*

(i) Una clase $ob\,\mathbf{C}$ *de objetos (normalmente denotados como* A*,* B*,* C*, etc.).*

(ii) Para cada par ordenado de objetos (A, B)*, un conjunto* $\hom_{\mathbf{C}}(A, B)$ *(donde* $\mathbf{C}$ *se puede omitir si no hay posibilidad de confusión). Los elementos de este conjunto se dirán morfismos con dominio* A *y codominio* B *o simplemente morfismos de* A *a* B*.*

(iii) Para cada trío de objetos (A, B, C)*, una aplicación* $(f, g) \mapsto gf$ *del conjunto producto* $\hom(A, B) \times \hom(B, C)$ *en* $\hom(A, C)$*.*

Se asume que tanto los objetos como los morfismos satisfacen las siguientes condiciones:

C1. Si $(A, B) \neq (C, D)$*, entonces* $\hom(A, B)$ *y* $\hom(C, D)$ *deben ser disjuntos.*

C2. (Asociatividad) Si $f \in \hom(A, B)$*,* $g \in \hom(B, C)$ *y* $h \in \hom(C, D)$*, entonces* $(hg)f = h(gf)$*. (De forma más simple, escribiremos* hgf*.)*

C3. (Existencia de unidad) Para cada objeto A*, existe un único elemento unidad* $1_A \in \hom(A, A)$ *tal que* $f1_A = f$ *para todo* $f \in \hom(A, B)$ *y* $1_A g = g$ *para todo* $g \in \hom(B, A)$*.*

Como notación, para indicar que $f \in \hom(A, B)$, escribiremos $f : A \to B$ o $A \xrightarrow{f} B$ y diremos a veces que f es una *flecha de* A *a* B. Además, cuando se especifiquen relaciones entre morfismos, normalmente no se usarán igualdades como en *C2* y *C3*, sino diagramas. Esta notación permite que dichas relaciones, sobre todo cuando sean más complejas, tengan un carácter más visual y sean más fáciles de comprender. Por ejemplo, la condición de asociatividad *C2*, $(hg)f = h(gf)$ puede expresarse diciendo que el siguiente diagrama

$$\begin{tikzcd}
A \arrow[d, "f"'] \arrow[dr] & D \\
B \arrow[r, "g"'] \arrow[ur] & C \arrow[u, "h"']
\end{tikzcd}$$

debe ser conmutativo para todo $f \in \hom(A, B)$ y $g \in \hom(B, C)$. La condición *C3* se expresará afirmando que existe un único elemento $1_A \in \hom(A, A)$ tal que el siguiente diagrama

$$\begin{tikzcd}
& B \arrow[dl, "g"'] \arrow[d, "g"] \\
A \arrow[r, "1_A"'] \arrow[dr, "f"'] & A \arrow[d, "f"] \\
& B
\end{tikzcd}$$

es conmutativo para todo $f \in \hom(A, B)$ y $g \in \hom(B, A)$.

Definición 3.2 (Subcategoría)**.** *Una categoría* $\mathbf{D}$ *es además una subcategoría de* $\mathbf{C}$ *si ob* $\mathbf{D}$ *es una subclase de ob* $\mathbf{C}$ *y para cada* $A, B \in$ *ob* $\mathbf{C}$*,* $\hom_{\mathbf{D}}(A, B) \subseteq \hom_{\mathbf{C}}(A, B)$*. La subcategoría* $\mathbf{D}$ *se dirá además completa si* $\hom_{\mathbf{D}}(A, B) = \hom_{\mathbf{C}}(A, B)$ *para todo par* $A, B \in$ *ob* $\mathbf{D}$*.*

Por la definición anterior de categoría, es obvio que la existencia de unidad se debe cumplir en $\mathbf{D}$ y el producto de morfismos ha de existir y ser el mismo que en $\mathbf{C}$.

Un ejemplo de categoría que más adelante usaremos es **Grp**, la categoría de los grupos. Para construirla definiremos ob **Grp** como la clase de todos los grupos existentes, $\hom(G, H)$ para dos grupos G y H como el conjunto de homomorfismos de grupos de G a H y el producto categórico como la composición de homomorfismos. A partir de esto, los axiomas de la definición de categoría se verifican de forma trivial si consideramos $1_G \in \hom(G, G)$ como el homomorfismo identidad en el grupo G.

Una subcategoría de **Grp** que más adelante resultará interesante es **Ab**, la categoría de los grupos abelianos. Con una construcción similar a la anterior es obvio que **Ab** es una categoría, en concreto, una subcategoría completa de **Grp**. Es también obvio que los módulos a izquierda sobre un anillo R que hemos introducido en la sección anterior se pueden agrupar en la categoría R-**mod**, definida de manera similar a las dos anteriores.

Hay ciertas formas generales de definir nuevas categorías a partir de otras ya existentes. En este trabajo serán de interés dos construcciones genéricas que se presentan a continuación: las categorías duales y las categorías producto.

Definición 3.3 (Categoría dual). *La categoría dual* $\mathbf{C}^{\mathbf{op}}$ *de otra categoría* $\mathbf{C}$ *se construye como ob* $\mathbf{C}^{\mathbf{op}}$ *= ob* $\mathbf{C}$*,* $\hom_{\mathbf{C}^{\mathbf{op}}}(A, B) = \hom_{\mathbf{C}}(B, A)$ *para cada par de objetos* A*,* B *y si* $f \in \hom_{\mathbf{C}^{\mathbf{op}}}(A, B)$ *y* $g \in \hom_{\mathbf{C}^{\mathbf{op}}}(B, C)$*, entonces* gf *(en* $\mathbf{C}^{\mathbf{op}}$*)* $= fg$ *(en* $\mathbf{C}$*).*

La prueba de que lo anterior efectivamente define una categoría es bastante sencilla. Este concepto es básicamente un "opuesto" a nivel categórico: respecto a los diagramas de morfismos (flechas), si se tiene que $A \xrightarrow{f} B$ en $\mathbf{C}$, entonces $A \xleftarrow{f} B$ en $\mathbf{C}^{\mathbf{op}}$ y si

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

es conmutativo en $\mathbf{C}$, entonces

$$\begin{tikzcd} A & B \arrow[l, "f"'] \\ & C \arrow[u, "g"'] \arrow[ul, "h"] \end{tikzcd}$$

es conmutativo en $\mathbf{C}^{\mathbf{op}}$. De forma más general, cualquier diagrama conmutativo en $\mathbf{C}$ da lugar a otro en $\mathbf{C}^{\mathbf{op}}$ al dar la vuelta a todas las flechas.

Definición 3.4 (Categoría producto). *Sean* $\mathbf{C}$ *y* $\mathbf{D}$ *dos categorías. Podemos definir la categoría producto* $\mathbf{C} \times \mathbf{D}$ *de la siguiente forma:* ob $\mathbf{C} \times \mathbf{D}$ = ob $\mathbf{C} \times$ ob $\mathbf{D}$*; si* A, B *son objetos de* $\mathbf{C}$ *y* A', B' *objetos de* $\mathbf{D}$*, entonces* $\hom_{\mathbf{C}\times\mathbf{D}}((A, A'), (B, B')) = \hom_{\mathbf{C}}(A, B) \times \hom_{\mathbf{D}}(A', B')$ *con* $1_{(A,A')} = (1_A, 1_{A'})$*, y si* $f \in \hom_{\mathbf{C}}(A, B)$*,* $g \in \hom_{\mathbf{C}}(B, C)$*,* $f' \in \hom_{\mathbf{D}}(A', B')$ *y* $g' \in \hom_{\mathbf{D}}(B', C')$ *entonces* $(g, g')(f, f') = (gf, g'f')$*.*

De la misma forma que antes, es obvio que esta construcción define una categoría. Es más, se puede obtener la categoría producto de una familia cualquiera de conjuntos generalizando la definición anterior, aunque no lo haremos aquí ya que no se necesitará más adelante.

3.2. Conceptos categóricos básicos

Comenzaremos esta sección presentando unos conceptos muy usados relativos a los morfismos de una categoría.

Definición 3.5 (Definiciones sobre morfismos)**.** *Sea* $\mathbf{C}$ *una categoría y sean* A*,* B *objetos de* $\mathbf{C}$*. Entonces:*

(i) Un morfismo $f : A \to B$ *se dice isomorfismo si existe un* $g : B \to A$ *de forma que* $fg = 1_B$ *y* $gf = 1_A$*.*

(ii) Si $f : A \to B$ *y* $g : B \to A$ *cumplen que* $gf = 1_A$ *entonces* f *se llama sección de* g *y* g *retracción de* f*.*

(iii) Un morfismo $f : A \to B$ *se dirá monomorfismo si es cancelable a izquierda en* $\mathbf{C}$*. Es decir, si* $g_1, g_2 \in \hom(C, A)$ *para cualquier objeto* C *y* $fg_1 = fg_2$*, entonces* $g_1 = g_2$*.*

(iv) Un morfismo $f : A \to B$ *se dirá epimorfismo si es cancelable a derecha en* $\mathbf{C}$*. Es decir, si* $g_1, g_2 \in \hom(B, C)$ *para cualquier objeto* C *y* $g_1 f = g_2 f$*, entonces* $g_1 = g_2$*.*

De estas definiciones se obtiene lo siguiente de forma inmediata:

Proposición 3.6. *Sea* $\mathbf{C}$ *una categoría y sean* A*,* B *objetos de* $\mathbf{C}$*. Entonces:*

(i) Si $A \xrightarrow{f} B$*,* $B \xrightarrow{g} C$ *y* f *y* g *son monomorfismos (epimorfismos) entonces* gf *es un monomorfismo (epimorfismo).*

(ii) Si $A \xrightarrow{f} B$*,* $B \xrightarrow{g} C$ *y* gf *es un monomorfismo (epimorfismo), entonces* f *es un monomorfismo (*g *es un epimorfismo).*

(iii) Si f *tiene una sección (retracción), entonces es un epimorfismo (monomorfismo).*

Estas definiciones de monomorfismo y epimorfismo no parecen a priori las que normalmente se usan en conjuntos, grupos u otras estructuras algebraicas corrientes. Sin embargo, en estas categorías habituales la definición que acaba de darse es equivalente a la que se usa normalmente:

Proposición 3.7. *Un morfismo* f *en* **Set***, la categoría de los conjuntos,* **Grp** *o* R*-***mod** *es un monomorfismo (epimorfismo) si y solamente si la aplicación que induce en el conjunto subyacente es inyectiva (sobreyectiva).*

Omitiremos la prueba de este resultado ya que no proporciona ninguna herramienta relevante para nuestro trabajo y también por su extensión, sobre todo en el caso de los grupos.

Muchas veces, un morfismo se dice inyectivo o suprayectivo cuando la aplicación subyacente lo es, para así simplificar el lenguaje y adecuarlo a lo usual. Podemos ver además que si bien la equivalencia anterior se da en bastantes categorías, no se da en todas. En otras tan usuales como **Ring**, categoría de los anillos unitarios, un morfismo es un monomorfismo si y solo si es inyectivo pero existen epimorfismos que no son sobreyectivos.

3.3. Funtores

Una de las herramientas más potentes de las que se dispone en la teoría de categorías son los *funtores*. Un funtor es básicamente un morfismo entre dos categorías, de forma que permite relacionar diversas estructuras (objetos de distintas categorías), trasladar conceptos y resultados de unas categorías a otras, etc. Su interés reside precisamente en esto, permitir "viajar" entre categorías permitiendo buscar mejores herramientas para resolver ciertos problemas o desarrollar teorías análogas en distintas estructuras algebraicas, geométricas o topológicas.

Definición 3.8 (Funtor covariante)**.** *Si $\mathbf{C}$ y $\mathbf{D}$ son dos categorías, un funtor (covariante) F de $\mathbf{C}$ a $\mathbf{D}$ consiste en*

(i) Una aplicación $A \mapsto FA$ de $\operatorname{ob}\mathbf{C}$ a $\operatorname{ob}\mathbf{D}$.

(ii) Para cada par de objetos (A, B) de $\mathbf{C}$, una aplicación $f \mapsto F(f)$ de $\hom_{\mathbf{C}}(A, B)$ a $\hom_{\mathbf{D}}(FA, FB)$.

Se requerirá además que un funtor satisfaga las dos siguientes condiciones:

F1. Si gf está definido en $\mathbf{C}$ para dos morfismos f y g, entonces la igualdad $F(gf) = F(g)F(f)$ debe cumplirse.

F2. $F(1_A) = 1_{FA}$.

La palabra "covariante" puede omitirse al hablar de este tipo de funtores, ya que son los más naturales. Sin embargo, a veces puede servir para distinguirlos bien de los *funtores contravariantes*. Un funtor contravariante de $\mathbf{C}$ a $\mathbf{D}$ es simplemente un funtor covariante de $\mathbf{C}^{\mathbf{op}}$ a $\mathbf{D}$. De esta forma, el punto (i) de la definición anterior se mantiene mientras que el segundo y la condición $F1$ se invierten. La aplicación entre morfismos ahora irá de $\hom_{\mathbf{C}}(A, B)$ a $\hom_{\mathbf{D}}(FB, FA)$ de forma que $F(gf) = F(f)F(g)$.

Un funtor permite trasladarse cómodamente entre categorías como antes hemos dicho porque conserva ciertas propiedades de una categoría a otra. Por ejemplo, es obvio que un funtor lleva los isomorfismos de la categoría original a isomorfismos de la categoría destino. Si en una categoría se tienen dos isomorfismos inversos f y g entre los objetos A y B (es decir, $fg = 1_B$ y $gf = 1_A$), entonces $F(f)F(g) = F(1_{FB}) = 1_{FB}$ y $F(g)F(f) = 1_{FA}$. De la misma forma, la imagen de una sección o una retracción será también una sección o una retracción. Sin embargo, no todo es tan sencillo: por ejemplo, el carácter de monomorfismo o epimorfismo no tiene por qué ser conservado por un funtor en general, para asegurar esto se necesita alguna condición más. Estas condiciones extras son las que llevan a la definición de la *equivalencia de categorías*, concepto muy importante ya que permite mover problemas y resultados entre categorías presentando muy pocas restricciones.

Un tipo concreto de funtores que más adelante nos serán de bastante utilidad son los *funtores exactos*. Estos funtores, los cuales cumplen que si $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ es una sucesión exacta corta, $0 \longrightarrow FM' \xrightarrow{F(f)} FM \xrightarrow{F(g)} FM'' \longrightarrow 0$ también lo es, son bastante poco comunes. Sí son más comunes los funtores que cumplen una condición algo más débil, en concreto que si $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ es una sucesión exacta corta, $0 \longrightarrow FM' \xrightarrow{F(f)} FM \xrightarrow{F(g)} FM''$ es también exacta. Estos últimos funtores se dicen *exactos a izquierda*, y de forma análoga se definen los *exactos a derecha*.

Respecto a las categorías producto, a un funtor de una categoría $\mathbf{B} \times \mathbf{C}$ a otra $\mathbf{D}$ se le suele llamar *bifuntor*. Los bifuntores pueden combinarse con los funtores contravariantes dando lugar por ejemplo a un funtor de $\mathbf{B^{op}} \times \mathbf{C}$ a $\mathbf{D}$, "contravariante en $\mathbf{B}$ y covariante en $\mathbf{C}$".

3.4. Los funtores hom

A continuación, definiremos unos funtores muy importantes de una categoría $\mathbf{C}$ y las relacionadas $\mathbf{C^{op}}$ y $\mathbf{C^{op}} \times \mathbf{C}$ a la categoría de los conjuntos $\mathbf{Set}$, relacionados con los morfismos de dicha categoría.

Antes de nada, clarifiquemos en qué consiste la categoría $\mathbf{C^{op}} \times \mathbf{C}$. En ella, los objetos son los pares (A, B) donde $A, B \in \text{ob}\,\mathbf{C}$; los morfismos entre dos objetos (A, B) y (A', B') de esta categoría son pares (f, g) donde $f : A' \to A$ y $g : B \to B'$, y por último, si (f', g') es otro morfismo de (A', B') a (A'', B'') de forma que $f' : A'' \to A'$ y $g' : B' \to B''$, entonces $(f', g')(f, g) = (ff', g'g)$. Además, como es natural, $1_{(A,B)} = (1_A, 1_B)$.

Podemos definir ahora el funtor hom de $\mathbf{C^{op}} \times \mathbf{C}$ a $\mathbf{Set}$ de forma que el objeto (A, B) tenga por imagen a $\hom(A, B)$ (un conjunto y por tanto un objeto de $\mathbf{Set}$) y el morfismo $(f, g) : (A, B) \to (A', B')$ tenga como imagen la aplicación $\hom(f, g)$ de $\hom(A, B)$ en $\hom(A', B')$ tal que $\hom(f, g) : k \mapsto gkf$. Nótese que esta última definición es correcta ya que como $f : A' \to A$, $g : B \to B'$ y $k : A \to B$, entonces la composición gkf lleva el conjunto A' al B'.

Comprobar que efectivamente lo anterior define un funtor es inmediato, ya que si $(f, g) : (A, B) \to (A', B')$ y $(f', g') : (A', B') \to (A'', B'')$, entonces $(f', g')(f, g) = (ff', g'g)$ y la condición *F1* se satisface ya que

$$\begin{aligned}\hom(ff', g'g)(k) = (g'g)k(ff') = g'(gkf)f' = \\ = g' \hom(f, g)(k)f' = \hom(f', g')(\hom(f, g)(k)),\end{aligned}$$

es decir, $\hom(f', g') \hom(f, g) = \hom((f', g')(f, g))$. Además, si $f = 1_A$ y $g = 1_B$, entonces $\hom(1_A, 1_B) : k \to 1_B k 1_A = k$, con lo que $\hom(1_A, 1_B)$ es la aplicación identidad en el conjunto $\hom(A, B)$ y *F2* se satisface. De esta forma, lo anteriormente definido es en efecto un bifuntor de $\mathbf{C}^{\mathbf{op}} \times \mathbf{C}$ a **Set**.

Si ahora fijamos un objeto A en $\mathbf{C}$, podemos definir un funtor $\hom(A, -)$ de $\mathbf{C}$ a **Set** mediante las siguientes transformaciones: $\hom(A, -)B = \hom(A, B)$ para todo $B \in \text{ob } \mathbf{C}$ y si g es un morfismo de B a B', entonces $\hom(A, -)(g)$ es la aplicación $\hom(A, g) : k \mapsto gk$ de $\hom(A, B)$ en $\hom(A, B')$. Es obvio, por un razonamiento similar al anterior, que esto define un funtor, al que llamaremos *funtor hom (covariante) dado por el objeto A*.

De forma similar definimos el *funtor hom contravariante dado por B* ($B \in \text{ob } \mathbf{C}$) como un funtor de $\mathbf{C}$ a **Set** de forma que $\hom(-, B)A = \hom(A, B)$ para todo $A \in \text{ob } \mathbf{C}$ y si f es un morfismo de A' en A, $\hom(-, B)(f)$ es la aplicación $\hom(f, B) : k \mapsto kf$ de $\hom(A, B)$ en $\hom(A', B)$.

Como última nota a esta sección, remarcaremos un resultado que posteriormente será de interés: los funtores hom (tanto covariantes como contravariantes) son funtores exactos a izquierda. Esta última propiedad no se probará aquí para no extendernos demasiado pero no es complicada de demostrar.

3.5. Categorías aditivas y abelianas

El desarrollo del álgebra homológica que se hará en la próxima sección se aplica en gran parte a un tipo "especial" de categorías, las *categorías abelianas*. Aunque por simplicidad normalmente se hable de módulos en dicha sección, un caso particular de categoría abeliana, será interesante disponer de algunas de las propiedades más básicas de las categorías abelianas en general. Es por eso que se introducen en este último apartado antes de pasar a la parte de homología del trabajo.

Las categorías abelianas son a su vez un tipo de *categorías aditivas*, por lo que este último será el concepto que primero se defina. Sin embargo, antes de hacerlo se necesita la noción de *objeto cero* y *morfismo cero*:

Definición 3.9 (Objeto cero). *Un objeto* 0 *de una categoría* $\mathbf{C}$ *se dice objeto cero si para cualquier objeto* A *de* $\mathbf{C}$*, los conjuntos* $\hom_{\mathbf{C}}(A, 0)$ *y* $\hom_{\mathbf{C}}(0, A)$ *constan de un solo elemento (es decir, si solo existe un morfismo* $A \to 0$ *y otro* $0 \to A$*).*

Definición 3.10 (Morfismo cero). *Si* A *y* B *son objetos de una categoría* $\mathbf{C}$ *con un objeto cero* 0*, definimos el morfismo cero de* A *a* B *como* $0_{A,B} := 0_{0,B} 0_{A,0}$ *donde* $0_{A,0}$ *es el único morfismo en* $\hom_{\mathbf{C}}(A, 0)$ *y* $0_{0,B}$ *el único morfismo en* $\hom_{\mathbf{C}}(0, B)$*.*

Es trivial ver que si 0 y $0'$ son objetos cero de una categoría, entonces existe un único isomorfismo entre ellos. De esta forma, el morfismo cero $0_{A,B}$ antes definido entre dos categorías es independiente del objeto cero elegido para construirlo.

Después de dar estas dos nociones, ya estamos en disposición de dar la definición de categoría aditiva:

Definición 3.11 (Categoría aditiva). *Una categoría* $\mathbf{C}$ *se dice aditiva si satisface las siguientes condiciones:*

CA1. $\mathbf{C}$ *tiene un objeto cero.*

CA2. Para cada par de objetos (A, B) *de* $\mathbf{C}$*, se puede definir una operación binaria* $+$ *en* $\hom(A, B)$ *de forma que* $(\hom(A, B), +, 0_{A,B})$ *tenga estructura de grupo abeliano.*

CA3. Si $A, B, C \in \mathrm{ob}\,\mathbf{C}$*,* $f, f_1, f_2 \in \hom(A, B)$ *y* $g, g_1, g_2 \in \hom(B, C)$*, entonces*

$$(g_1 + g_2)f = g_1 f + g_2 f$$
$$g(f_1 + f_2) = gf_1 + gf_2,$$

es decir, que el producto categórico entre morfismos es biaditivo.

CA4. Para cualquier familia finita de objetos $\{A_1, ..., A_n\}$ *existe un objeto* A *y una familia de morfismos* $p_j : A \to A_j$*,* $i_j : A_j \to A$*,* $1 \leq j \leq n$ *tales que*

$$p_j i_j = 1_{A_j}, \quad p_k i_j = 0 \text{ si } j \neq k, \quad \sum i_j p_j = 1_A.$$

En una categoría aditiva no solo tenemos una estructura de grupo definida a partir de *CA2*, sino que *CA3* implica que para cualquier objeto A, $(\hom_{\mathbf{C}}(A, A), +, \cdot, 0, 1)$, donde $\cdot$ es el producto categórico de morfismos, $0 = 0_{A,A}$ y $1 = 1_A$, tiene una estructura de anillo unitario (que es lo usual en muchas categorías habituales).

Es interesante remarcar, aunque aquí no se demostrará por no alargar demasiado este apartado, que si las cuatro condiciones anteriores se cumplen para una categoría $\mathbf{C}$ también lo hacen para la dual $\mathbf{C}^{\mathbf{op}}$. Esta "autodualidad" implica que $\mathbf{C}$ es una categoría aditiva si y solamente si su dual también lo es.

Las particularidades de las que las categorías aditivas disponen hacen que en ciertos momentos su tratamiento sea ligeramente especial. Por ejemplo, debido a la estructura de grupo abeliano existente en los grupos de morfismos $\hom(A, B)$ entre dos objetos de la categoría A y B, los funtores entre categorías aditivas se suelen asumir *aditivos* en el sentido de que la aplicación que el funtor F induce entre $\hom(A, B)$ y $\hom(FA, FB)$ sea un homomorfismo de grupos. En concreto los funtores hom sobre categorías aditivas serán aditivos, y se puede considerar la categoría de destino de estos funtores como **Ab** en vez de **Set** (debido a la estructura de grupo abeliano en los conjuntos de morfismos). Esta propiedad se aplicará más adelante al tratar con funtores hom sobre las categorías aditivas $R-\mathbf{mod}$ y su dual $\mathbf{mod}-R$ (las cuatro condiciones anteriores se verifican casi trivialmente para estas categorías).

Antes de definir la noción de categoría abeliana es necesario introducir dos conceptos más:

Definición 3.12 (Núcleo de un morfismo). *En una categoría* $\mathbf{C}$ *con objeto cero* 0*, sea* $f : A \to B$ *un morfismo. Entonces, un monomorfismo* $k : K \to A$ *será un núcleo de* f *si* $fk = 0$ *y para todo* $g : G \to A$ *tal que* $fg = 0$*, existe un* g' *tal que* $g = kg'$ *(y además, como* k *es monomorfismo, este* g' *será único).*

De esta forma, la última condición que el morfismo anterior k debe cumplir para ser un núcleo se puede expresar también diciendo que si el triángulo derecho en el diagrama

$$\begin{tikzcd}
K \arrow[r, "k"] & A \arrow[r, "f"] & B \\
& G \arrow[ul, dashed, "g'"] \arrow[u, "g"] \arrow[ur, "0"'] &
\end{tikzcd}$$

es conmutativo, entonces el diagrama puede completarse con un $g' : G \to K$ para obtener un diagrama completamente conmutativo. Es obvio a partir de esto que si k y k' son núcleos de f, existirá un único isomorfismo u tal que $k' = ku$.

Dualizando esta última definición se tiene que, bajo las mismas condiciones anteriores, un *conúcleo de* f es un epimorfismo $c : B \to C$ tal que $cf = 0$ y para cada $h : B \to C'$ tal que $hf = 0$, existe un h' tal que $h = h'c$. Esta última condición se puede expresar también dualizando el diagrama anterior.

Para ver que estas nociones no difieren demasiado de las normalmente usadas, nos centraremos un momento en la categoría $R-\mathbf{mod}$. Tomemos un morfismo $f : A \to B$ en esta categoría y sea $K = \ker f$ según la definición usual de núcleo. Veamos que k, la inclusión de K en A, es un núcleo de f y el homomorfismo canónico $c : B \to C = B/fA$ es un conúcleo de f.

Comencemos por k. Es obvio que k es un monomorfismo y $fk = 0$. Además, si g es un homomorfismo de G en A tal que $fg = 0$, entonces $gG \subseteq K$. De esta forma si tomamos g' como la restricción de g con codominio $K \subseteq A$, se tendrá que $g = kg'$. Como las tres propiedades se cumplen, k es efectivamente un núcleo de f. Por otro lado, c es obviamente un epimorfismo y cumple $cf = 0$. Además, si $h : B \to H$ cumple $hf = 0$, entonces $fA \subseteq \ker h$. De esta forma, podemos establecer un homomorfismo $h' : C = B/fA \to H$ tal que $h'c = h$ y se concluye que c es un conúcleo de f.

Después de este trabajo previo, ya estamos en condiciones de dar la definición de categoría abeliana:

Definición 3.13 (Categoría abeliana)**.** *Una categoría* $\mathbf{C}$ *se dice abeliana si es una categoría aditiva que cumple las siguientes propiedades adicionales:*

CA5. *Todo morfismo en* $\mathbf{C}$ *tiene un núcleo y un conúcleo.*

CA6. *Todo monomorfismo es un núcleo de su conúcleo y todo epimorfismo un conúcleo de su núcleo.*

CA7. *Todo morfismo puede descomponerse como* $f = me$ *donde* e *es un epimorfismo y* m *un monomorfismo.*

Con lo previo a esta definición ya se ha visto que $R-\mathbf{mod}$ cumple *CA5*. La prueba para *CA6* (similar a la de *CA7*) es algo más complicada y no se incluye aquí por no hacer demasiado extensa esta sección, pero se puede probar que $R-\mathbf{mod}$ es una categoría abeliana.

4. Introducción al álgebra homológica

Como adelantamos en la introducción del trabajo, desde que el álgebra homológica comenzó su desarrollo a mediados del siglo XX se ha convertido en una de las áreas más importantes del álgebra. En este capítulo presentaremos las herramientas homológicas más básicas, con un desarrollo orientado a que en la siguiente sección se pueda hablar de dos de las aplicaciones más importantes de esta teoría.

En primer lugar se necesita completar el estudio de los módulos proyectivos e inyectivos que se dejó en el aire en el apartado 2.4, ya que el conocimiento del lenguaje de categorías hace que este estudio sea mucho más fácil. Una vez completado este punto, se habrá terminado de introducir toda la teoría previa que es necesaria para hablar de homología.

Para desarrollar la introducción al álgebra homológica que se da en esta sección, nos centraremos en estudiar esta teoría para el caso concreto de los módulos. Ya hemos visto al final de la sección anterior que los módulos forman un caso particular de categoría abeliana, y debemos comentar que el álgebra homológica puede extenderse a cualquier categoría abeliana y desarrollarse genéricamente. Si el tratamiento de este tema que se incluye en esta sección solo recoge el caso de los módulos es debido a que en primer lugar, desarrollar genéricamente el álgebra homológica es una tarea que necesita un trabajo más extenso. Además en el contexto de este trabajo no se obtiene ninguna ganancia con el desarrollo para una categoría abeliana más allá de la de los módulos, ya que con lo que se verá a continuación se tiene todo lo necesario para desarrollar las aplicaciones presentadas en la siguiente sección.

De esta forma, comenzaremos la sección definiendo los conceptos homológicos más básicos haciendo hincapié en el más importante, los complejos. A continuación hablaremos de otras herramientas que nos permitirán seguir avanzando hacia el punto final y más importante de la sección: la construcción de los funtores derivados. Estas herramientas son la sucesión exacta larga de homología y las resoluciones de módulos, hablando también de la relación de homotopía, que más adelante cobrará su importancia, como previo a las resoluciones. Por último, definiremos la noción de funtor derivado y nos centraremos en unos muy particulares, relacionados con las extensiones de ciertas estructuras algebraicas: los funtores Ext.

En esta sección no se han tenido que dejar fuera muchos de los puntos que se consideran básicos en el álgebra homológica, pero construcciones tan importantes como el funtor Tor (derivado del producto tensorial, que tampoco pudo verse) y resultados tan conocidos como el Teorema de la Base de Hilbert se han tenido que omitir.

4.0. Previo: sobre módulos proyectivos e inyectivos

Como paso previo al desarrollo del álgebra homológica, vamos a profundizar un poco más en las nociones de proyectividad e inyectividad para módulos. Como ya se comentó en el apartado 2.4, si esto se ha preferido desarrollar aquí es porque el trabajo con este tipo de módulos es mucho más sencillo de hacer una vez se conoce el lenguaje categórico.

Aunque no se comentó en su momento, los módulos libres presentan una interesante propiedad de "elevación": si F es un módulo libre y tenemos el siguiente diagrama

$$\begin{tikzcd} & F \arrow[d, "\bar{f}"] \\ M \arrow[r, two heads, "\lambda"] & M' \end{tikzcd}$$

(donde la flecha con dos cabezas representa un epimorfismo), el diagrama se puede completar con un homomorfismo $f : M \to F$ obteniendo un triángulo conmutativo. La prueba es muy sencilla, si X es una base para F, para cada $x \in X$ tomamos un $m \in M$ tal que $\lambda m = \bar{f}x$ (lo cual se puede hacer por ser λ epimorfismo). Además, sea f el homomorfismo de F a M tal que $fx = m$. Entonces, $\lambda f x = \bar{f}x$ para todo $x \in X$ de donde se puede seguir que $\lambda f = \bar{f}$, como queríamos obtener.

Quedándonos solamente con esta propiedad de elevación de los módulos libres, definimos los módulos proyectivos como sigue:

Definición 4.1 (Módulo proyectivo)**.** *Un módulo P se dice proyectivo si dado cualquier diagrama*

$$\begin{tikzcd} & P \arrow[d, "f"] \\ M \arrow[r, two heads, "\lambda"] & M' \end{tikzcd}$$

existe un homomorfismo $g : P \to M$ tal que

$$\begin{tikzcd} & P \arrow[d, "f"] \arrow[dl, dashed, "g"'] \\ M \arrow[r, two heads, "\lambda"] & M' \end{tikzcd}$$

es conmutativo. O dicho de otra forma, si dado cualquier epimorfismo $p : M \to M'$, todo homomorfismo $f : P \to M'$ se puede factorizar como $f = pg$ para algún $g : P \to M$.

Por la definición es obvio que todo módulo libre es proyectivo (básicamente surgen como una generalización de los primeros), pero en general el recíproco no es cierto.

A continuación daremos tres propiedades (es más, tres caracterizaciones) de los módulos proyectivos que nos serán de gran utilidad más adelante.

Proposición 4.2. *Un módulo P es proyectivo si y solamente si* $\hom(P,-)$ *es un funtor exacto.*

Demostración. Como se comentó en el apartado 3.4, para cualquier módulo P el funtor $\hom(P,-)$ es exacto a izquierda. Entonces, si $0 \to N' \xrightarrow{i} N \xrightarrow{p} N'' \to 0$ es una sucesión exacta, entonces podemos asegurar que

$$0 \longrightarrow \hom(P,N') \xrightarrow{\hom(P,i)} \hom(P,N) \xrightarrow{\hom(P,p)} \hom(P,N'')$$

es también exacta. Pero si además P es proyectivo, dado un $f \in \hom(M,N'')$, existe un $g \in \hom(P,N)$ tal que $\hom(P,p)(g) = pg = f$. De esta forma $\hom(P,p)$ es sobreyectivo y con ello se tiene la exactitud de

$$0 \longrightarrow \hom(P,N') \xrightarrow{\hom(P,i)} \hom(P,N) \xrightarrow{\hom(P,p)} \hom(P,N'') \longrightarrow 0,$$

probando así la exactitud del funtor $\hom(P,-)$.

Para la implicación inversa, supongamos que $\hom(P,-)$ es un funtor exacto y que $p : M \to N$ es un epimorfismo. Denotemos $K = \ker p$. Entonces, la sucesión $0 \to K \xrightarrow{i} M \xrightarrow{p} N \to 0$ donde i es la inclusión de K en M es exacta. Si aplicamos ahora la exactitud de $\hom(P,-)$, tenemos que

$$0 \longrightarrow \hom(P,K) \xrightarrow{\hom(P,i)} \hom(P,M) \xrightarrow{\hom(P,p)} \hom(P,N) \longrightarrow 0$$

es también exacta y en concreto la aplicación $\hom(P,p)$ de $\hom(P,M)$ en $\hom(P,N)$ es sobreyectiva. De esta forma, todo $f \in \hom(P,N)$ se podrá escribir como $f = pg$ para un cierto $g \in \hom(P,M)$, obteniendo precisamente la definición de proyectividad. Entonces P es proyectivo. □

Antes de dar las dos siguientes caracterizaciones, necesitamos una noción previa sobre sucesiones exactas cortas:

Definición 4.3 (Sucesión exacta corta escindible)**.** *Una sucesión exacta corta $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ se dice escindible o que se escinde si existe un $i' : M'' \to M$ tal que $pi' = 1_{M''}$ o, equivalentemente, si existe un $p' : M \to M'$ tal que $p'i = 1_{M'}$.*

La relevancia de este tipo de sucesiones la da la siguiente propiedad: si una sucesión exacta corta como la de la definición anterior se escinde, entonces $M \cong M' \oplus M''$. Probar esto no es complicado, pero nuevamente se omite en este trabajo por tema de extensión.

Proposición 4.4. *Las siguientes afirmaciones sobre un módulo P son equivalentes:*

(i) P es proyectivo.

(ii) Cualquier sucesión exacta corta $0 \to M \to N \to P \to 0$ se escinde.

(iii) P es sumando directo de un módulo libre (es decir, existe un módulo libre F isomorfo a $P \oplus P'$ para algún P').

Demostración. $(i) \Rightarrow (ii)$. Sea $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ una sucesión exacta y consideremos el diagrama

$$\begin{tikzcd} & P \arrow[d, "1_P"] \\ N \arrow[r, two heads, "g"] & P \end{tikzcd}$$

Como P es proyectivo por hipótesis, este diagrama se puede completar con un homomorfismo $g' : P \to N$ obteniendo un diagrama conmutativo. Entonces, $gg' = 1_P$ y por tanto la sucesión dada se escinde.

$(ii) \Rightarrow (iii)$. No es complicado ver que un módulo cualquiera puede verse como la imagen por un homomorfismo de un módulo libre. De esta forma, podemos construir una sucesión exacta $0 \to P' \xrightarrow{i} F \xrightarrow{p} P \to 0$ donde F es un módulo libre. Por hipótesis, esta sucesión se escinde y entonces $F \cong P \oplus P'$.

$(iii) \Rightarrow (i)$. Como el módulo libre F es isomorfo a $P \oplus P'$ por hipótesis, podemos construir una sucesión exacta $0 \to P' \xrightarrow{i} F \xrightarrow{p} P \to 0$ que se escinde. Consideremos ahora el siguiente diagrama:

$$\begin{tikzcd} & P \arrow[d, "f"] \\ M \arrow[r, two heads, "q"'] & N. \end{tikzcd}$$

Además, debido a que la sucesión anterior se escinde sabemos que existe un homomorfismo $i' : P \to F$ tal que $pi' = 1_P$. Combinando la sucesión anterior, este último diagrama y el homomorfismo i', tenemos que:

$$\begin{tikzcd} 0 \arrow[r] & P' \arrow[r, "i"] & F \arrow[r, shift left, "p"] \arrow[dr, "fp"'] & P \arrow[l, shift left, "i'"] \arrow[r] \arrow[d, "f"] & 0 \\ & & M \arrow[r, two heads, "q"'] & N. & \end{tikzcd}$$

Como F es libre, es también proyectivo, de forma que podemos completar lo anterior con un homomorfismo $g : F \to M$ para obtener un "triángulo" conmutativo tal que $fp = qg$. Entonces, $f = f1_P = fpi' = qgi'$ y la existencia de este homomorfismo $gi' : P \to M$ tal que $f = qgi'$ significa que el siguiente diagrama

$$\begin{tikzcd} & P \arrow[dl, "gi'"'] \arrow[d, "f"] \\ M \arrow[r, two heads, "q"'] & N. \end{tikzcd}$$

es conmutativo para cualquier $f \in \hom(P, N)$ y q epimorfismo de M en N, luego P es proyectivo. $\square$

Como consecuencia de este resultado tenemos otro que también nos será de interés más adelante:

Corolario 4.5. *Sea $\{A_i\}_{i\in I}$ una familia de R-módulos. Entonces $A = \oplus_{i\in I} A_i$ es proyectivo si y solamente si todos los A_i son proyectivos.*

Demostración. Para la implicación directa, supongamos que A es proyectivo y sea $j \in I$. Por el resultado anterior, existe un R-módulo K tal que $F = A \oplus K$ es libre. Pero entonces $F \cong A_j \oplus (\oplus_{i\in I, i\neq j} A_i \oplus K)$ y entonces A_j es proyectivo nuevamente por el resultado anterior. Supongamos ahora que todos los A_i son proyectivos. Entonces, para cada $i \in I$ existe un R-módulo K_i tal que $F_i = A_i \oplus K_i$ es libre. Sea $F = \oplus_{i\in I} F_i$ y $K = \oplus_{i\in I} K_i$. Entonces F será un R-módulo libre tal que $F = A \oplus K$ y por el resultado anterior, A será proyectivo. $\square$

Como dualización de los módulos proyectivos surgen los *módulos inyectivos*. Por razones de extensión y como más adelante nos centraremos en trabajar con los primeros, no nos alargaremos demasiado hablando este tipo de módulos, sino que solo daremos una definición y un par de propiedades interesantes sin demostrar.

Definición 4.6 (Módulo inyectivo)**.** *Un módulo Q se dice inyectivo si dado cualquier diagrama de homomorfismos de módulos*

$$\begin{tikzcd} N \arrow[r, tail, "i"] \arrow[d, "f"] & M \\ Q & \end{tikzcd}$$

(donde la flecha con una cabeza al inicio y otra al final representa un monomorfismo), existe otro homomorfismo $g : M \to Q$ que completa el diagrama anterior y lo hace conmutativo. En otras palabras, dado un $f : N \to Q$ y un monomorfismo $i : N \to M$ existe un $g : M \to Q$ tal que $f = gi$.

Obviamente, como la noción de inyectividad es dual a la de proyectividad, se pueden obtener caracterizaciones dualizando las dadas para módulos proyectivos. En concreto, un módulo Q será inyectivo si y solamente si el funtor hom contravariante $\hom(-, Q)$ es exacto o si y solamente si cualquier sucesión exacta corta de la forma $0 \to Q \to M \to N \to 0$ se escinde. Sin embargo, aunque estos resultados son los duales de los vistos para módulos proyectivos y enunciarlos es fácil, probarlos (en concreto el segundo) no es tan trivial. Su prueba se basa en el siguiente teorema cuya demostración no es inmediata y es demasiado extensa para incluirla aquí:

Teorema 4.7. *Cualquier módulo puede ser encajado en un módulo inyectivo.*

Este teorema da además una de las propiedades más interesantes de los módulos inyectivos, sabiendo además que lo podemos refinar y afirmar que existe un encaje o, visto al revés, una extensión inyectiva “mínima” que es única salvo isomorfismos.

En general, los módulos inyectivos surgen como la generalización de los números racionales (vistos como un $\mathbb{Z}$-módulo) ya que la inyectividad se relaciona bastante estrechamente con la divisibilidad, no son una simple dualización de los proyectivos sin mayor interés. Sin embargo, esto se escapa ya del contexto de este trabajo.

4.1. Conceptos básicos de homología. Complejos

En este apartado y los que siguen se irán introduciendo una tras otra las herramientas más importantes del álgebra homológica básica, culminando en la definición de los funtores derivados en el apartado 4.5. Como se ha indicado antes, aunque esta teoría se puede desarrollar para cualquier categoría abeliana, aquí nos centraremos en desarrollarla para R-módulos (y por tanto, también para grupos abelianos como caso particular $R = \mathbb{Z}$). La primera noción y la más básica en este tema es la de complejo:

Definición 4.8 (Complejo). *Sea R un anillo. Un complejo (C, d) sobre R (o R-complejo) es una familia de R-módulos $C = \{C_i\}_{i\in\mathbb{Z}}$ junto con una familia de R-homomorfismos $d = \{d_i : C_i \to C_{i-1}\}_{i\in\mathbb{Z}}$, tales que $d_{i-1}d_i = 0$ para todo i entero.*

Esta definición permite representar un complejo usando la misma notación que en anteriores apartados hemos usado para las sucesiones exactas. Un complejo (C, d) se puede escribir por tanto como:

$$\cdots \longrightarrow C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1} \longrightarrow \cdots .$$

Notemos que aunque en principio la sucesión dada por un complejo no tenga por qué ser exacta, bajo ciertos supuestos que veremos más adelante sí que lo será.

Definición 4.9 (Homomorfismo entre complejos). *Si (C, d) y (C', d') son dos R-complejos, un homomorfismo de C a C' es una familia de homomorfismos de módulos $\alpha = \{\alpha_i : C_i \to C'_i\}_{i\in\mathbb{Z}}$ tal que el diagrama*

$$\begin{array}{ccc} C_i & \xrightarrow{d_i} & C_{i-1} \\ {\scriptstyle\alpha_i}\downarrow & & \downarrow{\scriptstyle\alpha_{i-1}} \\ C'_i & \xrightarrow[d'_i]{} & C'_{i-1} \end{array}$$

es conmutativo para todo i entero. Esta condición se suele resumir como $\alpha d = d'\alpha$.

De forma bastante natural, estas últimas dos definiciones permiten introducir una nueva categoría, R**-comp**, de complejos sobre el anillo R. Sus objetos son los R-complejos (C, d) y para cada par de objetos (C, d), (C', d'), el conjunto $\hom(C, C')$ comprende los homomorfismos $(C, d) \to (C', d')$ de acuerdo a la última definición. Esta construcción define efectivamente una categoría que además se puede ver que es abeliana, aunque esto no se probará en detalle.

Los complejos aparecerán con más interés en los siguientes apartados de esta sección y por usar una notación más sucinta a veces serán denotados solamente como $C = (C, d)$. Sin embargo, ciertos conceptos básicos deben ser introducidos antes de poder seguir desarrollando más teoría. En concreto, llegaremos ahora a la definición de *funtor de homología* de forma constructiva, intentando que surja de la manera más natural posible.

Si (C, d) es un complejo, denotaremos para cada i entero $Z_i(C) := \ker d_i$, un submódulo de C_i. Como $d_i d_{i+1} = 0$, es obvio que la imagen $d_{i+1}C_{i+1}$ es un submódulo de $Z_i(C)$, el cual denotaremos como $B_i(C)$. A los elementos de $Z_i(C)$ les denominaremos *i-ciclos* y a los de $B_i(C)$, *i-bordes*, nombres que cobrarán sentido cuando veamos sus aplicaciones a la topología algebraica. De esta forma, podemos definir el *i-ésimo módulo de homología H_i* para el complejo C (o "grupo" si $R = \mathbb{Z}$) como $H_i(C) = Z_i(C)/B_i(C)$. Estos módulos además dan una condición sobre cuándo la sucesión determinada por el complejo (C, d) es exacta: es obvio que $C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1}$ será exacta si y solo si $d_{i+1}C_{i+1} = \ker d_i$, es decir, si $B_i(C) = Z_i(C)$ y en este caso $H_i(C) = 0$. Extendiendo esto, se tiene que

$$\cdots \longrightarrow C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1} \longrightarrow \cdots$$

será exacta si y solamente si $H_i(C) = 0$ para todo i.

Sea ahora α un homomorfismo del complejo (C, d) en otro (C', d'). Entonces, recordando que para todo i entero, $\alpha_{i-1}d_i = d'_i\alpha_i$, tenemos que $\alpha_i Z_i(C) \subseteq Z_i(C')$ y que $\alpha_i B_i(C) \subseteq B_i(C')$. De esta forma la aplicación $z_i \mapsto \alpha_i z_i + B_i(C')$, define un homomorfismo de $Z_i(C)$ en $H_i(C') = Z_i(C')/B_i(C')$ tal que la imagen de $B_i(C)$ es 0. Esto permite definir el homomorfismo $\widetilde{\alpha}_i$ de $H_i(C)$ en $H_i(C')$ tal que $z_i + B_i(C) \mapsto \alpha_i z_i + B_i(C')$.

De esta forma, hemos encontrado tanto una aplicación del complejo (C, d) en el módulo $H_i(C)$ como otra del conjunto $\hom(C, C')$ en $\hom(H_i(C), H_i(C'))$ tal que $\alpha \mapsto \widetilde{\alpha}_i$. La comprobación de que estas dos aplicaciones definen un funtor de R-**comp** a R-**mod** es trivial, y a este funtor se le dice normalmente *i-ésimo funtor de homología*. Además, puesto que $\alpha \mapsto \widetilde{\alpha}_i$ es un homomorfismo de grupos abelianos (R-**mod** es una categoría abeliana como ya hemos visto y se puede probar que R-**comp** también lo es), el i-ésimo funtor de homología es aditivo.

En la mayoría de ejemplos que más adelante encontraremos, los complejos que aparezcan cumplirán que $C_i = 0$ para todo $i < 0$ o para todo $i > 0$. En el primer caso, a estos complejos se les dice *positivos* o *complejos de cadenas*, mientras que en el segundo se les dice *negativos* o *complejos de cocadenas*. En este último caso, para no complicar la notación se suele escribir $C^i := C_{-i}$, $d^i := d_{-i}$ y $H^i := H_{-i}$. De esta forma, un complejo de cadenas será de la forma $0 \longleftarrow C_0 \xleftarrow{d_1} C_1 \xleftarrow{d_2} C_2 \longleftarrow \cdots$ y uno de cocadenas $0 \longrightarrow C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^2} C^2 \longrightarrow \cdots$.

4.2. Sucesión exacta larga de homología

En esta sección se construirá otra herramienta homológica más: la *sucesión exacta larga de homología* que surge a partir de una sucesión exacta corta de complejos.

Definición 4.10 (Sucesión exacta corta de complejos). *Una sucesión de complejos y homomorfismos entre ellos $C' \xrightarrow{\alpha} C \xrightarrow{\beta} C''$ se dice sucesión exacta corta de complejos* *si para todo $i \in \mathbb{Z}$, la sucesión de módulos $0 \longrightarrow C_i' \xrightarrow{\alpha_i} C_i \xrightarrow{\beta_i} C_i'' \longrightarrow 0$ es exacta (es decir, α_i inyectiva, β_i sobreyectiva y $\ker \beta_i = \operatorname{im} \alpha_i$). Como notación, se dirá en este caso que $0 \longrightarrow C' \longrightarrow C \longrightarrow C'' \longrightarrow 0$ es exacta.*

De esta forma se tiene para cada i el siguiente diagrama conmutativo con filas exactas,

$$\begin{tikzcd}
0 \arrow[r] & C'_{i+1} \arrow[r, "\alpha_{i+1}"] \arrow[d, "d'_{i+1}"'] & C_{i+1} \arrow[r, "\beta_{i+1}"] \arrow[d, "d_{i+1}"'] & C''_{i+1} \arrow[r] \arrow[d, "d''_{i+1}"'] & 0 \\
0 \arrow[r] & C'_{i} \arrow[r, "\alpha_{i}"] \arrow[d, "d'_{i}"'] & C_{i} \arrow[r, "\beta_{i}"] \arrow[d, "d_{i}"'] & C''_{i} \arrow[r] \arrow[d, "d''_{i}"'] & 0 \\
0 \arrow[r] & C'_{i-1} \arrow[r, "\alpha_{i-1}"] & C_{i-1} \arrow[r, "\beta_{i-1}"] & C''_{i-1} \arrow[r] & 0,
\end{tikzcd}$$

a partir del cual queremos definir una sucesión exacta larga de la siguiente forma:

Teorema 4.11 (Sucesión exacta larga de homología)**.** *Sea $0 \to C_i' \xrightarrow{\alpha} C \xrightarrow{\beta} C'' \to 0$ una sucesión exacta corta de complejos. Entonces, para cada $i \in \mathbb{Z}$ podemos definir un homomorfismo de módulos $\Delta_i : H_i(C'') \to H_{i-1}(C')$ de forma que la sucesión infinita de módulos de homología*

$$\cdots \longrightarrow H_i(C') \xrightarrow{\tilde{\alpha}_i} H_i(C) \xrightarrow{\tilde{\beta}_i} H_i(C'') \xrightarrow{\Delta_i} H_{i-1}(C') \xrightarrow{\tilde{\alpha}_{i-1}} H_{i-1}(C) \longrightarrow \cdots$$

sea exacta.

Este homomorfismo Δ_i se llama *homomorfismo de conexión* de $H_i(C'')$ a $H_{i-1}(C')$ y la sucesión anterior es la *sucesión exacta larga de homología* determinada por la sucesión exacta corta de complejos $0 \longrightarrow C' \xrightarrow{\alpha} C \xrightarrow{\beta} C'' \longrightarrow 0$.

4.3. Homotopía

Como ya hemos visto, un homomorfismo α de un complejo (C, d) a otro (C', d') determina un homomorfismo $\widetilde{\alpha}_i : H_i(C) \to H_i(C')$ entre sus i-ésimos módulos de homología para cada $i \in \mathbb{Z}$. Resulta que bajo ciertas condiciones, los homomorfismos entre los módulos de homología correspondientes a dos homomorfismos de complejos distintos son iguales. Estas condiciones se recogen en la siguiente definición:

Definición 4.12 (Homomorfismos homotópicos)**.** *Sean α y β homomorfismos de un complejo (C, d) en otro (C', d'). Entonces, diremos que α y β son homotópicos y lo denotaremos como $\alpha \sim \beta$ si existe una familia $s = \{s_i : C_i \to C'_{i+1}\}_{i \in \mathbb{Z}}$ de homomorfismos de módulos tal que*

$$\alpha_i - \beta_i = d'_{i+1} s_i + s_{i-1} d_i$$

para todo i entero.

Por no complicar la notación, supondremos en lo que sigue que $Z_i = Z_i(C)$ y $Z'_i = Z_i(C')$. Simplificaremos también la notación para los B_i y H_i de forma análoga.

Veamos que efectivamente si $\alpha \sim \beta$, entonces los homomorfismos correspondientes entre los módulos de homología cumplen $\widetilde{\alpha}_i = \widetilde{\beta}_i$, como hemos indicado al comienzo de este apartado. Si $z_i \in Z_i$, entonces $z_i + B_i \in H_i$ y se cumple que $\widetilde{\alpha}_i(z_i + B_i) = \alpha_i z_i + B'_i$ y $\widetilde{\beta}_i(z_i + B_i) = \beta_i z_i + B'_i$. Entonces,

$$\begin{aligned}\widetilde{\alpha}_i(z_i + B_i) &= \alpha_i z_i + B'_i = (\beta_i + d'_{i+1}s_i + s_{i-1}d_i)z_i + B'_i \\ &= (\beta_i z_i + d'_{i+1}s_i z_i) + B'_i = \beta_i z_i + B'_i = \tilde{\beta}_i(z_i + B_i),\end{aligned}$$

ya que como $z_i \in Z_i = \ker d_i$, $s_{i-1}d_i z_i = 0$ y $d'_{i+1}s_i z_i \in d'_{i+1}C'_{i+1} = B'_i$, lo que prueba el resultado deseado.

Las bondades de la homotopía no solo quedan en lo anterior: la homotopía constituye una relación de equivalencia. La simetría y reflexividad son triviales y no merecen una prueba detallada. Con respecto a la transitividad, si la relación $\alpha \sim \beta$ viene dada por la familia de homomorfismos s y $\beta \sim \gamma$ viene dada por t, entonces

$$\begin{aligned}\alpha_i - \beta_i &= d'_{i+1}s_i + s_{i-1}d_i \\ \beta_i - \gamma_i &= d'_{i+1}t_i + t_{i-1}d_i,\end{aligned}$$

de donde sumando se llega a

$$\begin{aligned}\alpha_i - \gamma_i &= d'_{i+1}s_i + s_{i-1}d_i + d'_{i+1}t_i + t_{i-1}d_i \\ &= d'_{i+1}(s_i + t_i) + (s_{i-1} + t_{i-1})d_i\end{aligned}$$

y por tanto $s + t = \{s_i + t_i\}$ define una relación de homotopía entre α y γ. Incluso se puede probar que la composición (de homomorfismos de complejos) preserva las relaciones de homotopía de forma similar a lo que se acaba de hacer, por lo que la prueba no se incluirá aquí.

4.4. Resoluciones de módulos

Hablaremos ahora de otra de las herramientas necesarias para seguir dándole más fuerza al álgebra homológica: las resoluciones de módulos. Este concepto nos llevará a definir los funtores derivados en la próxima sección, que más tarde se revestirán de una gran importancia.

Definición 4.13 (Complejo sobre un módulo)**.** *Sea M un R-módulo. Se define C, ε, complejo sobre M, como un complejo positivo $C = (C, d)$ junto con un homomorfismo de "aumentación" $\varepsilon : C_0 \to M$ tal que $\varepsilon d_1 = 0$. De esta forma, se tiene la siguiente sucesión de homomorfismos de módulos*

$$\cdots \longrightarrow C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots \longrightarrow C_1 \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

donde la composición de dos homomorfismos sucesivos cualesquiera es igual a 0. El complejo se dice además proyectivo si todos los C_i son a su vez proyectivos.

A partir de esta definición se puede dar la de resolución como sigue:

Definición 4.14 (Resolución de un módulo)**.** *Un complejo C, ε sobre M se denomina resolución de M si la sucesión de homomorfismos de módulos*

$$\cdots \longrightarrow C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots \longrightarrow C_1 \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

es exacta. De forma equivalente, C, ε será una resolución de M si para todo $i > 0$, $H_i(C) = 0$ y $H_0(C) = C_0/d_1C_1 = C_0/\ker\varepsilon \cong M$. Nuevamente, dicha resolución se dirá proyectiva si todos los C_i son proyectivos.

La existencia de una resolución proyectiva de un módulo se puede comprobar de una forma bastante sencilla. Es más, veremos que existe una resolución de un módulo cualquiera M que puede decirse *libre*, en el sentido de que todos los módulos C_i que la componen son libres. Para ello, representamos M como la imagen por un homomorfismo (más concretamente, epimorfismo) ε de un módulo libre C_0 (recordamos que esto siempre se puede hacer), obteniendo así la sucesión exacta

$$\ker\varepsilon \xrightarrow{i} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0,$$

donde C_0 es libre e i denota la inclusión de $\ker\varepsilon$ en C_0. A continuación, se puede tomar un módulo libre C_1 y un epimorfismo π de C_1 en $\ker\varepsilon$. Si definimos $d_1 = i\pi : C_1 \to C_0$, obtendremos la sucesión

$$C_1 \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0,$$

que será exacta ya que la imagen de d_1 será la misma que la de i, $\ker\varepsilon$. Iterando este proceso, vemos que podemos construir (y que por tanto existe) una sucesión exacta de la forma

$$\cdots \longrightarrow C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots \longrightarrow C_1 \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0,$$

donde los C_i son libres y (C, d) junto con ε conforman una resolución libre para M.

Se tiene el siguiente resultado, bastante importante, sobre resoluciones y complejos proyectivos:

Teorema 4.15. *Sea C, ε un complejo proyectivo sobre el módulo M y sea C', ε' una resolución del módulo M'. Además, sea μ un homomorfismo cualquiera de M en M'. Entonces, existe un homomorfismo α del complejo C al complejo C' (es decir, una familia de homomorfismos $\{\alpha_i\}$ de los C_i a los C'_i) tal que $\mu\varepsilon = \varepsilon'\alpha_0$. Además, si otro homomorfismo β cumple esta condición, entonces es homotópico a α.*

Demostración. La condición dada en las hipótesis se puede expresar como que existen homomorfismos α_i, $i \geq 0$ tales que el siguiente diagrama con la fila inferior exacta

$$\begin{tikzcd}
\cdots \arrow[r] & C_n \arrow[r, "d_n"] \arrow[d, dashed, "\alpha_n"'] & C_{n-1} \arrow[r, "d_{n-1}"] \arrow[d, dashed, "\alpha_{n-1}"'] & C_{n-2} \arrow[r] \arrow[d, dashed, "\alpha_{n-2}"'] & \cdots \arrow[r] & C_0 \arrow[r, "\varepsilon"] \arrow[d, dashed, "\alpha_0"'] & M \arrow[r] \arrow[d, "\mu"'] & 0 \\
\cdots \arrow[r] & C'_n \arrow[r, "d'_n"] & C'_{n-1} \arrow[r, "d'_{n-1}"] & C'_{n-2} \arrow[r] & \cdots \arrow[r] & C'_0 \arrow[r, "\varepsilon'"] & M' \arrow[r] & 0
\end{tikzcd}$$

sea conmutativo. Veamos que esto efectivamente ocurre. Como C_0 es un módulo proyectivo y $C'_0 \xrightarrow{\varepsilon'} M' \to 0$ es una sucesión exacta, el homomorfismo $\mu\varepsilon : C_0 \to M'$ puede ser descompuesto mediante otro homomorfismo $\alpha_0 : C_0 \to C'_0$ de forma que $\mu\varepsilon = \varepsilon'\alpha_0$. Procedamos ahora por inducción, suponiendo que se han determinado unos $\alpha_0, ..., \alpha_{n-1}$ de forma que la conmutatividad del diagrama anterior se tiene hasta la columna $n-1$. Sabemos que $d'_{n-1}\alpha_{n-1}d_n = \alpha_{n-2}d_{n-1}d_n = 0$. Entonces, $\alpha_{n-1}d_nC_n \in \ker d'_{n-1} = \operatorname{im} d'_n = d'_nC_n$. Así, podemos reemplazar C'_{n-1} por $d'_nC'_n$, obteniendo la exactitud de $C'_n \to d'_nC'_n \to 0$. Por la proyectividad de C_n, existirá un homomorfismo $\alpha_n : C_n \to C'_n$ tal que $d'_n\alpha_n = \alpha_{n-1}d_n$, completando el último paso de la inducción y demostrando así que el homomorfismo de complejos α del teorema efectivamente existe. Para completar la prueba, sean ahora α y β dos homomorfismos de complejos satisfaciendo las condiciones dadas en la tesis del teorema y veamos que $\alpha \sim \beta$. Sea $\gamma = \alpha - \beta$. Entonces, tenemos que

$$\begin{aligned} &\varepsilon'\gamma_0 = \varepsilon'\alpha_0 - \varepsilon'\beta_0 = \mu\varepsilon - \mu\varepsilon = 0, \text{ y} \\ &d'_n\gamma_n = \gamma_{n-1}d_n \end{aligned}$$

para todo $n \geq 1$. Tenemos entonces el diagrama

$$\begin{tikzcd} & C_0 \arrow[d, "\gamma_0"] & & \\ C'_1 \arrow[r, "d'_1"] & C'_0 \arrow[r, "\varepsilon'"] & M' \arrow[r] & 0, \end{tikzcd}$$

y como además $\varepsilon'\gamma_0 = 0$, $\gamma_0C_0 \subseteq d'_1C'_1$, podemos reducir el diagrama a otro

$$\begin{tikzcd} & C_0 \arrow[d, "\gamma_0"] & \\ C'_1 \arrow[r, "d'_1"] & d'_1C'_1 \arrow[r] & 0 \end{tikzcd}$$

cuya fila inferior es exacta. Como C_0 es proyectivo, existe un homomorfismo $s_0 : C_0 \to C'_1$ tal que $\gamma_0 = d'_1s_0$. Para proceder nuevamente por inducción, supongamos ahora que hemos determinado los homomorfismos $s_0, ..., s_{n-1}$ tales que $s_i : C_i \to C'_{i+1}$ y

$$\gamma_i = d'_{i+1}s_i + s_{i-1}d_i$$

para todo i, $0 \leq i \leq n-1$. Consideremos ahora $\gamma_n - s_{n-1}d_n$. Tenemos que $d'_n(\gamma_n - s_{n-1}d_n) = \gamma_{n-1}d_n - d'_ns_{n-1}d_n = (\gamma_{n-1} - d'_ns_{n-1})d_n = s_{n-2}d_{n-1}d_n = 0$. De aquí se sigue como antes que por ser C_n proyectivo, existirá un homomorfismo $s_n : C_n \to C'_{n+1}$ tal que $d'_{n+1}s_n = \gamma_n - s_{n-1}d_n$. Entonces, por inducción podemos asegurar que la familia de homomorfismos $\{s_i\}_{i\in\mathbb{Z}}$ define una homotopía entre α y β, completando así la demostración. □

Al anterior homomorfismo α entre los complejos C y C', el cual aparece de forma recurrente en homología, se le suele decir *homomorfismo en cadena sobre μ*.

Para terminar esta sección, recordamos que como muchos otros conceptos anteriores, el de resolución puede dualizarse. De esta forma un *complejo bajo M* se define como un par D, η donde D es un complejo negativo y η es un homomorfismo de M a D^0 tal que $d^0\eta = 0$. Tal complejo bajo M se dirá *corresolución* de M si $0 \longrightarrow M \xrightarrow{\eta} D^0 \xrightarrow{d^0} D^1 \xrightarrow{d^1} \cdots$ es una sucesión exacta. Además, se puede hablar de *corresoluciones inyectivas* en un sentido similar al que hablamos de resoluciones proyectivas y dar un resultado dual al anterior.

4.5. Funtores derivados

Después de todos los conceptos que han sido previamente introducidos en esta sección, estamos ya en disposición de introducir una de las herramientas más importantes dentro del álgebra homológica: los funtores derivados de un funtor aditivo. Nuevamente, aunque para esta sección podríamos estudiar los funtores entre categorías aditivas en general, nos centraremos en los funtores (aditivos) de la categoría R-**mod**, de los módulos sobre un anillo R, a la categoría **Ab** de los grupos abelianos.

Sea M un R-módulo y F un funtor aditivo de la categoría R-**mod** a la categoría **Ab**. Sea además

$$0 \longleftarrow M \xleftarrow{\varepsilon} C_0 \xleftarrow{d_1} C_1 \xleftarrow{d_2} \cdots$$

una resolución proyectiva de M. Aplicando el funtor F, obtendríamos una sucesión de homomorfismos de grupos abelianos como la que sigue,

$$0 \longleftarrow FM \xleftarrow{\varepsilon} FC_0 \xleftarrow{F(d_1)} FC_1 \xleftarrow{F(d_2)} \cdots .$$

Como $F(0) = 0$, entendiendo los ceros como homomorfismos nulos, y como F es además multiplicativo, el producto de homomorfismos sucesivos en el anterior diagrama será 0. Esto significa que $FC = \{FC_i\}$ junto con $F(d) = \{F(d_i)\}$ y la aumentación $F(\varepsilon)$ forman un complejo (positivo) sobre FM.

Además, si F es un funtor exacto, entonces la última sucesión es exacta y los grupos de homología $H_i(FC) = 0$ para $i \geq 1$. Si F no fuera exacto la sucesión no tendría por qué ser exacta, y en este caso, estos grupos de homología nos podrían dar una intuición de cuánto "se desvía" F de la exactitud.

A continuación, veremos constructivamente qué se entiende por un funtor derivado de F a partir de lo anterior. Para ello, definimos

$$L_nFM := H_n(FC)$$

para cualquier $n \geq 0$ (notemos que en el caso $i = 0$, $H_0(FC) = FC_0/F(d_1)FC_1$).

Sea ahora M' un segundo R-módulo y supongamos que hemos elegido una resolución proyectiva $0 \longleftarrow M' \xleftarrow{\varepsilon'} C'_0 \xleftarrow{d'_1} C'_1 \longleftarrow \cdots$ de donde obtenemos los grupos (abelianos) de homología $H_n(FC')$, $n \geq 0$. Tomamos ahora un homomorfismo μ de M a M', a partir del cual ya hemos visto que podemos determinar un homomorfismo en cadena α del complejo (C, d) al complejo (C', d') sobre μ (es decir, cumpliendo que $\mu\varepsilon = \varepsilon'\alpha_0$). Como F es un funtor aditivo, tendremos que $F(\alpha)$ es un homomorfismo del complejo FC en FC' tal que $F(\mu)F(\varepsilon) = F(\varepsilon')F(\alpha_0)$. De esta forma, el diagrama

$$\begin{tikzcd}
0 & FM \arrow[l] \arrow[d, "F(\mu)"'] & FC_0 \arrow[l, "F(\varepsilon)"'] \arrow[d, "F(\alpha_0)"'] & FC_1 \arrow[l, "F(d_1)"'] \arrow[d, "F(\alpha_1)"'] & \cdots \arrow[l] \\
0 & FM' \arrow[l] & FC'_0 \arrow[l, "F(\varepsilon')"] & FC'_1 \arrow[l, "F(d'_1)"] & \cdots \arrow[l]
\end{tikzcd}$$

es conmutativo.

Ahora, consideremos el homomorfismo $\widetilde{F}(\alpha_n)$ de $H_n(FC)$ a $H_n(FC')$ y veamos que dicho homomorfismo es independiente del anterior α elegido: si β fuera otro homomorfismo sobre μ de C a C', hemos visto en el apartado anterior que $\beta \sim \alpha$, así que existe una familia de homomorfismos $s_n : C_n \to C'_{n+1}$, $n \geq 0$, tal que

$$\alpha_n - \beta_n = d'_{n+1}s_n + s_{n-1}d_n.$$

Como F es aditivo, si aplicamos F a esta última relación se tiene que

$$F(\alpha_n) - F(\beta_n) = F(d'_{n+1})F(s_n) + F(s_{n-1})F(d_n),$$

por lo que $F(\alpha) \sim F(\beta)$ y de esa forma $\widetilde{F}(\alpha_n) = \widetilde{F}(\beta_n)$. A partir de esto, definimos

$$L_nF(\mu) := \widetilde{F}(\alpha_n).$$

De esta forma vemos que un homomorfismo $\mu \in \hom(M, M')$ determina otro homomorfismo $L_nF(\mu) \in (H_n(FC), H_n(FC')) = \hom(L_nFM, L_nFM')$.

Probar que L_nF a partir de esta construcción constituye un funtor aditivo es bastante directo. Por tanto, estamos ya en condiciones de poder dar la definición de funtor derivado como sigue:

Definición 4.16 (Funtor derivado)**.** *La aplicación L_nF que, según la construcción anterior, se define como*

$$\begin{aligned} (L_nF)M &= H_n(FC), \qquad && M \in \operatorname{ob} R-\mathbf{mod} \\ (L_nF)(\mu) &= \widetilde{F}(\alpha_n), \qquad && \mu \in \hom(M, M'), \end{aligned}$$

*constituye un funtor aditivo de $R-$**mod** a **Ab** denominado n-ésimo funtor derivado (a izquierda) del funtor aditivo F.*

Por último, veamos que los funtores derivados son totalmente independientes de las resoluciones elegidas para construirlos como antes hemos hecho. Sea entonces $\bar{C}, \bar{\varepsilon}$ otra resolución proyectiva de M. Entonces, tomando $\mu = 1$ en la construcción anterior obtendríamos una familia única de isomorfismos $\{\eta_n\}_{n\geq 0}$, $\eta_n : H_n(FC) \to H_n(F\bar{C})$. Además, otra resolución proyectiva de M', $\bar{C}', \bar{\varepsilon}'$, nos daría otra familia única de isomorfismos $\{\eta'_n\}$ de $H_n(FC')$ a $H_n(F\bar{C}')$. Esto nos permitiría sustituir el funtor L_nF por otro similar $\eta'_n(L_nF)\eta_n^{-1}$.

De esta forma, en lo que ahora sigue supondremos que para cada R-módulo M se han determinado los funtores derivados L_nF a partir de unas resoluciones en particular, pero podremos cambiar de una resolución a otra cuando sea conveniente.

Veremos a continuación un resultado sobre cómo los funtores derivados, junto con unos homomorfismos de conexión, permiten construir sucesiones exactas de grupos abelianos a partir de una sucesión exacta corta de módulos. Para ello, necesitamos en primer lugar introducir el siguiente concepto, generalizando el de resolución proyectiva de un módulo:

Definición 4.17 (Resolución proyectiva de una sucesión exacta corta)**.** *Se dice resolución proyectiva de una sucesión exacta corta* $0 \to M' \to M \to M'' \to 0$ *al trío de resoluciones proyectivas* C', ε', C, ε, C'', ε'' *de* M', M *y* M'' *respectivamente junto con unos homomorfismos de cadenas* $i : C' \to C$, $p : C \to C''$ *tales que para cada* n, $0 \to C'_n \to C_n \to C''_n \to 0$ *es exacta y*

$$\begin{tikzcd} C'_0 \arrow[r, "i_0"] \arrow[d, "\varepsilon'"'] & C_0 \arrow[r, "p_0"] \arrow[d, "\varepsilon"'] & C''_0 \arrow[d, "\varepsilon''"'] \\ M' \arrow[r, "\alpha"] & M \arrow[r, "\beta"] & M'' \end{tikzcd}$$

es conmutativo.

Veamos que efectivamente existe una resolución proyectiva para cualquier sucesión exacta corta de módulos $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$. Tomamos para ello dos resoluciones proyectivas, C', ε' y C'', ε'' de M' y M'' respectivamente:

$$\begin{aligned} \cdots \longrightarrow C'_2 \xrightarrow{d'_2} C'_1 \xrightarrow{d'_1} C'_0 \xrightarrow{\varepsilon'} M' \longrightarrow 0 \\ \cdots \longrightarrow C''_2 \xrightarrow{d''_2} C''_1 \xrightarrow{d''_1} C''_0 \xrightarrow{\varepsilon''} M'' \longrightarrow 0 \end{aligned} \tag{1}$$

Definimos ahora $C_n = C'_n \oplus C''_n$ para todo $n \geq 1$ y construimos los homomorfismos i, p de la definición como $i_n x'_n = (x'_n, 0)$ y $p_n x_n = x''_n$ para todo $x'_n \in C'_n$ y $x_n = (x'_n, x''_n) \in C_n$. De esta forma ya tenemos cumplida la condición de que para cada n, la sucesión $0 \to C'_n \xrightarrow{i} C_n \xrightarrow{p} C''_n \to 0$ sea exacta ya que i es una familia de monomorfismos, p de epimorfismos y $p_n i_n = 0$ para todo n. Además, los $C_n = C'_n \oplus C''_n$ son todos proyectivos por ser suma directa de otros módulos proyectivos.

Faltan por definir ahora los homomorfismos $\varepsilon : C_0 \to M$ y $d_n : C_n \to C_{n-1}$ de forma que C, ε sea una resolución de M y se cumplan las condiciones sobre el rectángulo de la definición anterior. Para ello, y teniendo en cuenta que para todo n, $x_n = (x'_n, x''_n)$, tomaremos $\varepsilon x_0 = \alpha \varepsilon' x'_0 + \sigma x''_0$ y $d_n x_n = (d'_n x'_n + \theta_n x''_n, d''_n x''_n)$, con $\sigma : C''_0 \to M'$ y $\theta_n : C''_n \to C'_{n-1}$ a determinar de forma que se cumplan las condiciones que se acaban de mencionar.

En primer lugar, la conmutatividad de la parte izquierda del rectángulo de la definición se tiene directamente, ya que $\varepsilon i_0 x'_0 = \varepsilon(x'_0, 0) = \alpha \varepsilon' x'_0$ para todo $x'_0 \in C'_0$. Para la parte derecha, tenemos que $\varepsilon'' p_0 x_0 = \varepsilon'' x''_0$ y $\beta \epsilon x_0 = \beta(\alpha \varepsilon' x'_0 + \sigma x''_0) = \beta \sigma x''_0$ ya que $\beta\alpha = 0$. De esta forma, la conmutatividad en la parte derecha del rectángulo se tendrá si y solamente si

$$\varepsilon'' = \beta \sigma. \tag{2}$$

Por otro lado, para que C, ε sea una resolución de M, se necesita en principio que $\varepsilon d_1 = 0$. Tenemos que para todo $x_1 \in C_1$, $\varepsilon d_1 x_1 = \varepsilon(d_1' x_1' + \theta_1 x_1'', d_1'' x_1'') = \alpha\varepsilon'\theta_1 x_1'' + \sigma d_1'' x_1''$. De esta forma $\varepsilon d_1 = 0$ si y solo si

$$\alpha\varepsilon'\theta_1 + \sigma d_1'' = 0. \tag{3}$$

Por último, para que C, ε sea una resolución también se necesita que $d_{n-1}d_n = 0$ para todo $n > 1$. Por la definición antes dada de los d_n, esta condición es equivalente a que para todo $n > 1$,

$$d_{n-1}'\theta_n + \theta_{n-1}d_n'' = 0. \tag{4}$$

Consideremos ahora el diagrama

$$\begin{tikzcd}
& C_0'' \arrow[dl, dashed, "\sigma"'] \arrow[d, "\varepsilon''"] & \\
M \arrow[r, "\beta"'] & M'' \arrow[r] & 0.
\end{tikzcd}$$

Como C_0'' es proyectivo y la fila de abajo exacta, existe un $\sigma : C_0'' \to M$ tal que (2) se cumple, con lo que tenemos la conmutatividad de todo el rectángulo en la definición. A continuación, construimos el siguiente diagrama

$$\begin{tikzcd}
& C_1'' \arrow[dl, dashed, "\theta_1"'] \arrow[d, "-\sigma d_1''"] & \\
C_0' \arrow[r, "\alpha\varepsilon'"'] & M \arrow[r, "\beta"'] & M''
\end{tikzcd}$$

en donde, como $\varepsilon' C_0' = M'$, la fila inferior es exacta. Además, debido a la proyectividad de C_1'' y que $\beta\sigma d_1'' = \varepsilon'' d_1'' = 0$, entonces existe un $\theta_1 : C_1'' \to C_0'$ tal que (3) se cumple (es decir, $\alpha\varepsilon'\theta_1 = -\sigma d_1''$). Considerando el siguiente diagrama similar al anterior,

$$\begin{tikzcd}
& C_2'' \arrow[dl, dashed, "\theta_2"'] \arrow[d, "-\theta_1 d_2''"] & \\
C_1' \arrow[r, "d_1'"'] & C_0' \arrow[r, "\varepsilon'"'] & M',
\end{tikzcd}$$

tenemos que la fila inferior vuelve a ser exacta, C_2'' es proyectivo y $\varepsilon'\theta_1 d_2'' = 0$ ya que $\alpha\varepsilon'\theta_1 d_2'' = -\sigma d_1'' d_2'' = 0$ y α es un monomorfismo. Entonces, con este diagrama se prueba que existe un $\theta_2 : C_2'' \to C_1'$ tal que (4) se cumple para $n = 2$. Mediante inducción y usando el diagrama

$$\begin{tikzcd}
& C_n'' \arrow[dl, dashed, "\theta_n"'] \arrow[d, "-\theta_{n-1} d_n''"] & \\
C_{n-1}' \arrow[r, "d_{n-1}'"'] & C_{n-2}' \arrow[r, "d_{n-2}'"'] & C_{n-3}'
\end{tikzcd}$$

se prueba fácilmente que (4) se cumple para todo $n > 1$.

Falta ver, por último, que $\cdots \longrightarrow C_2 \xrightarrow{d_2} C_1 \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0$ es, en efecto, una resolución. Para ello, denotaremos como $\bar{C}$ el complejo que forma esta sucesión de módulos y homomorfismos, así como $\bar{C}'$ y $\bar{C}''$ a los dos complejos que surgen de forma similar a partir de (1). De esta forma, hemos comprobado ya que $0 \to \bar{C}' \to \bar{C} \to \bar{C}'' \to 0$ es una sucesión exacta de complejos. Por el teorema 4.11, podemos construir entonces la sucesión exacta larga de homología,

$$\cdots \longrightarrow H_i(\bar{C}') \xrightarrow{\tilde{\alpha}_i} H_i(\bar{C}) \xrightarrow{\tilde{\beta}_i} H_i(\bar{C}'') \xrightarrow{\Delta_i} H_{i-1}(\bar{C}') \xrightarrow{\tilde{\alpha}_{i-1}} H_{i-1}(\bar{C}) \longrightarrow \cdots,$$

de la cual sabemos que $H_i(\bar{C}') = 0 = H_i(\bar{C}'')$ para todo i. Añadiendo esto a la exactitud de la sucesión anterior, podemos concluir que $H_i(\bar{C}) = 0$ para todo i y de esta forma, $\bar{C}$ es una resolución de M que junto con las resoluciones de M' y M'' en (1) forma una resolución proyectiva para la sucesión exacta corta $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$.

Una vez probada la existencia de una resolución proyectiva para cualquier sucesión exacta corta de módulos, estamos en disposición de probar el teorema al que antes se ha hecho alusión.

Teorema 4.18. *Sea F un funtor aditivo de R-**mod** a **Ab**. Para cualquier sucesión exacta corta de R-módulos $0 \to M' \overset{\alpha}{\to} M \overset{\beta}{\to} M'' \to 0$ existe una familia de homomorfismos de conexión $\{\Delta_n : L_nFM'' \to L_{n-1}FM'\}_{n\geq 1}$, tal que*

$$0 \longleftarrow L_0FM'' \xleftarrow{L_0F(\beta)} L_0FM \xleftarrow{L_0F(\alpha)} L_0FM' \xleftarrow{\Delta_1} L_1FM'' \xleftarrow{L_0F(i_0)} \cdots$$

es exacta.

Demostración. En primer lugar se construye una resolución proyectiva C', ε', C, ε, C'', ε'', i, p para la sucesión exacta corta de módulos dada. Esto significa que para cada $n \geq 0$ se tendrá ahora la sucesión exacta corta

$$0 \longrightarrow C'_n \xrightarrow{i_n} C_n \xrightarrow{p_n} C''_n \longrightarrow 0.$$

Como C''_n es proyectivo, la sucesión anterior se escinde y consecuentemente,

$$0 \longrightarrow FC'_n \xrightarrow{F(i_n)} FC_n \xrightarrow{F(p_n)} FC''_n \longrightarrow 0$$

es exacta y se escinde. De esta forma, hemos conseguido una sucesión exacta corta de complejos

$$0 \longrightarrow F(C') \xrightarrow{F(i)} F(C) \xrightarrow{F(p)} F(C'') \longrightarrow 0.$$

Aplicando a esta sucesión el teorema 4.11 de la sucesión exacta larga de homología, se llega inmediatamente a la sucesión que da el resultado deseado. □

Como en otras ocasiones, acabaremos esta sección recordando que todo lo que se ha desarrollado en esta sección puede ser dualizado y aplicado a *corresoluciones*, obteniendo así tanto la definición de *funtores derivados a derecha* como resultados análogos sobre ellos.

4.6. Los funtores Ext

Ciertas familias de funtores derivados son muy interesantes y en esta sección se presenta una de ellas, los funtores Ext, que al hablar de las extensiones de grupos se harán totalmente necesarios. Estos funtores se definen a partir del funtor hom contravariante $\hom(-, N)$ determinado por un R-módulo N (recordemos que los funtores hom en las categorías que aquí manejamos son aditivos). Para poder obtener el funtor derivado que queremos, en primer lugar se deben aclarar los ligeros cambios que hay que hacer al procedimiento de la sección anterior, ya que ahora estamos usando funtores contravariantes de $R-\mathbf{mod}$ a $\mathbf{Ab}$ en contraposición a los covariantes anteriores.

Recordemos que un funtor contravariante es uno covariante de la categoría dual, en este caso de $R-\mathbf{mod}^{\mathrm{op}}$ a $\mathbf{Ab}$, y como al pasar a la categoría opuesta las flechas se invierten, también lo harán los roles de proyectividad e inyectividad de los módulos. De esta forma, para definir el funtor derivado (a derecha) de un funtor aditivo contravariante G de $R-\mathbf{mod}$ a $\mathbf{Ab}$, comenzamos con una resolución proyectiva $0 \longleftarrow M \xleftarrow{\varepsilon} C_0 \xleftarrow{d_1} C_1 \longleftarrow \cdots$ de un módulo M dado. De aquí se puede obtener la sucesión $0 \longrightarrow GM \xrightarrow{G(\varepsilon)} GC_0 \xrightarrow{G(d_1)} GC_1 \longrightarrow \cdots$ y el complejo de cocadenas $(GC, G(d))$, donde $GC = \{GC_i\}$ y $G(d) = \{G(d_i)\}$.

De forma similar a la sección anterior, podemos definir $(R^nG)M = H^n(GC)$. En particular, $(R^0G)M = \ker G(d_1)$. Además, para cada homomorfismo $\mu \in \hom_R(M', M)$, podemos construir otro homomorfismo $(R^nG)(\mu) : (R^nG)M \to (R^nG)M'$, obteniendo de esta forma el *n-ésimo funtor derivado a derecha* R^nG de G, que será aditivo y contravariante.

Usando el teorema 4.18 con los cambios antes propuestos, podemos afirmar que para cualquier sucesión exacta corta $0 \to M' \to M \to M'' \to 0$ se puede construir la *sucesión exacta larga de cohomología* como sigue,

$$0 \to R^0GM'' \to R^0GM \to R^0GM' \to R^1GM'' \to R^1GM \to \cdots ,$$

donde las flechas $R^nGM' \to R^{n+1}GM''$ están dadas por un homomorfismo de conexión. Lógicamente, la prueba es casi totalmente idéntica a la de dicho teorema, por lo que no se volverá a incluir.

Estudiemos ahora el caso particular $G = \hom(-, N)$, el funtor hom contravariante determinado por un R-módulo N fijo. Por definición,

$$\begin{aligned} \hom(-, N)M &= \hom_R(M, N), \quad && M \in \operatorname{ob} R-\mathbf{mod} \\ \hom(-, N)(\alpha) &= \alpha^*, && \alpha \in \hom_R(M, M') \end{aligned}$$

donde $\alpha^* : \hom_R(M', N) \to \hom_R(M, N)$, tal que $\alpha^*(\beta) = \beta\alpha$. Esta definición es correcta, ya que $\hom(-, N)M$ es un grupo abeliano para todo objeto M y α^* es un homomorfismo de grupos (a partir de esto vemos que efectivamente el funtor $\hom(-, N)$ es aditivo y también contravariante ya que $(\alpha_1\alpha_2)^* = \alpha_2^*\alpha_1^*$). Además, como ya se remarcó en el apartado 3.4, este funtor es exacto a izquierda, es decir, que si $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ es exacta, entonces

$$0 \longrightarrow \hom(M'', N) \xrightarrow{\hom(\beta,N)} \hom(M, N) \xrightarrow{\hom(\alpha,N)} \hom(M', N)$$

también lo es (la inversión de la sucesión se debe a que el funtor es contravariante).

De esta forma, el procedimiento de derivación de funtores a derecha presentado al inicio de este apartado es válido para el funtor $\hom(-, N)$, lo cual nos permite definir sus derivados como:

Definición 4.19 (Funtores Ext)**.** *El n-ésimo funtor derivado a derecha del funtor hom contravariante* $\hom(-, N)$ *dado por un R-módulo N fijo se denota como* $\mathrm{Ext}^n(-, N)$*(o* $\mathrm{Ext}^n_R(-, N)$ *si hace falta especificar el anillo R).*

De forma abreviada, el valor $\mathrm{Ext}^n(-, N)M$ para un R-módulo M se suele denotar como $\mathrm{Ext}^n(M, N)$, algo que también se hacía con el funtor hom de una forma similar. Una propiedad interesante de este grupo $\mathrm{Ext}^n(M, N)$ para el caso $n = 0$ es que $\mathrm{Ext}^0(M, N) \cong \hom(M, N)$.

En efecto, si C, ε es una resolución proyectiva para M, entonces la exactitud de la sucesión $C_1 \longrightarrow C_0 \xrightarrow{\varepsilon} M \longrightarrow 0$ implica la de $0 \longrightarrow \hom(M, N) \xrightarrow{\varepsilon^*} \hom(C_0, N) \longrightarrow \hom(C_1, N)$. Como $\mathrm{Ext}^0(M, N)$ es el núcleo del homomorfismo de $\hom(C_0, N)$ en $\hom(C_1, N)$, se tiene entonces que $\mathrm{Ext}^0(M, N) \cong \hom(M, N)$ bajo la aplicación ε^*.

Sea ahora $0 \to M' \to M \to M'' \to 0$ una sucesión exacta corta. Por el teorema 4.18 con los cambios antes descritos, a partir de ella podemos obtener la sucesión exacta larga

$$\begin{aligned} 0 &\to \mathrm{Ext}^0(M'', N) \to \mathrm{Ext}^0(M, N) \to \mathrm{Ext}^0(M', N) \\ &\to \mathrm{Ext}^1(M'', N) \to \mathrm{Ext}^1(M, N) \to \cdots , \end{aligned}$$

y si usamos aquí el isomorfismo anterior para el funtor Ext^0, podemos ver cómo la sucesión exacta $0 \to \hom(M'', N) \to \hom(M, N) \to \hom(M', N)$ se puede encajar en una sucesión exacta larga como sigue,

$$\begin{aligned} 0 &\to \hom(M'', N) \to \hom(M, N) \to \hom(M', N) \\ &\to \mathrm{Ext}^1(M'', N) \to \mathrm{Ext}^1(M, N) \to \cdots . \end{aligned} \tag{5}$$

Tras realizar todas las construcciones anteriores estamos en condiciones de probar el siguiente teorema:

Teorema 4.20 (Funtores Ext para módulos proyectivos)**.** *Las siguientes afirmaciones para un módulo M son equivalentes:*

(i) M *es proyectivo.*

(ii) $\mathrm{Ext}^n(M, N) = 0$ *para todo* $n \geq 1$ *y cualquier módulo* N*.*

(iii) $\mathrm{Ext}^1(M, N) = 0$ *para cualquier módulo* N*.*

Demostración. (i) $\Rightarrow$ (ii): Si M es proyectivo, entonces se comprueba inmediatamente que $0 \longleftarrow M \xleftarrow{1_M} C_0 = M \longleftarrow 0 \longleftarrow \cdots$ es una resolución proyectiva para M. El complejo correspondiente a la sucesión anterior, a partir del que se calculará $\operatorname{Ext}^n(M,N)$, es por tanto $0 \longrightarrow \hom(M,N) \longrightarrow \hom(M,N) \longrightarrow 0 \longrightarrow \cdots$, con lo que obviamente $\operatorname{Ext}^n(M,N) = 0$ para todo $n \geq 1$.
(ii) $\Rightarrow$ (iii): Trivial.
(iii) $\Rightarrow$ (i): Sea M un módulo cualquiera y sea $0 \to K \xrightarrow{\eta} P \xrightarrow{\varepsilon} M \to 0$ una sucesión exacta corta con P proyectivo. Entonces, por (5) y como $\operatorname{Ext}^1(P,N) = 0$, probado en la primera parte de esta demostración, se tiene la exactitud de

$$0 \longrightarrow \hom(M,N) \xrightarrow{\varepsilon *} \hom(P,N) \xrightarrow{\eta *} \hom(K,N) \longrightarrow \operatorname{Ext}^1(M,N) \longrightarrow 0.$$

Es más, teniendo en cuenta la hipótesis, tenemos demostrada la exactitud de

$$0 \longrightarrow \hom(M,N) \xrightarrow{\varepsilon *} \hom(P,N) \xrightarrow{\eta *} \hom(K,N) \longrightarrow 0,$$

lo que implica que la aplicación η^* de $\hom(P,N)$ en $\hom(K,N)$ es sobreyectiva. Sea ahora $N = K$ (ya que la hipótesis se cumple para cualquier N). Entonces, la sobreyectividad de η^* en $\hom(K,K)$ implica que existe un $\zeta \in \hom(P,K)$ tal que $1_K = \eta^*(\zeta) = \zeta\eta$. Esto implica que la sucesión exacta corta $0 \to K \xrightarrow{\eta} P \xrightarrow{\varepsilon} M \to 0$ se escinde y de esta forma M es un sumando directo de P, módulo proyectivo, con lo que M es también proyectivo. $\square$

Analicemos ahora un poco más la sucesión exacta corta usada antes, $0 \to K \xrightarrow{\eta} P \xrightarrow{\varepsilon} M \to 0$, con M un módulo arbitrario y P uno proyectivo. A partir de ella y con las construcciones de la demostración anterior se puede dar la siguiente fórmula:

$$\operatorname{Ext}^1(M,N) = \operatorname{coker} \eta^* = \hom(K,N)/\operatorname{im}(\hom(\eta,N)).$$

Esto nos servirá para relacionar el grupo $\operatorname{Ext}^1(M,N)$ con las *extensiones del módulo M por el módulo N*. De forma rigurosa, una extensión de módulos se define como:

Definición 4.21 (Extensión de módulos)**.** *Sean M y N dos módulos. Se define una extensión de M por N como una sucesión exacta corta $0 \to N \xrightarrow{\alpha} E \xrightarrow{\beta} M \to 0$, a la que nos referiremos por brevedad como "la extensión E".*

Es esta conexión entre el funtor Ext y las extensiones la que le da su nombre. Por otro lado, existe una relación de equivalencia entre estas extensiones que se presenta a continuación.

Definición 4.22 (Equivalencia de extensiones)**.** *Dos extensiones E_1 y E_2 se dirán equivalentes si existe un homomorfismo $\gamma : E_1 \to E_2$ tal que el diagrama*

$$\begin{tikzcd}
& E_1 \arrow[dd, "\gamma"] \arrow[dr, "\beta_1"] & \\
N \arrow[ur, "\alpha_1"] \arrow[dr, "\alpha_2"'] & & M \\
& E_2 \arrow[ur, "\beta_2"'] &
\end{tikzcd}$$

es conmutativo.

Es casi trivial ver que si γ es un homomorfismo de la extensión E_1 a la E_2 de forma que el diagrama anterior es conmutativo, entonces γ es además un isomorfismo de módulos. Esto implica que la equivalencia de extensiones es, efectivamente, una relación de equivalencia. Además, es obvio que las extensiones de un módulo M por otro N existen, ya que la *extensión escindible*

$$0 \longrightarrow N \xrightarrow{i} M \oplus N \xrightarrow{p} M \longrightarrow 0$$

con i la inclusión y p la proyección canónica claramente existe y ya ha sido usada en anteriores secciones de este trabajo.

En concreto, es en la equivalencia de extensiones donde el funtor Ext^1 entra en juego:

Teorema 4.23. *Para dos módulos M y N, existe una biyección entre* $\mathrm{Ext}^1(M, N)$ *y el conjunto de las clases de equivalencia de las extensiones de M por N.*

Este resultado no se probará aquí ya que la demostración es bastante extensa. Además, en este trabajo hemos preferido no centrarnos demasiado en las extensiones de módulos y sí desarrollar más adelante el problema de la extensión de grupos, donde también se puede apreciar la importancia del funtor Ext.

5. Dos aplicaciones del álgebra homológica

En esta última sección se presentan dos aplicaciones distintas del álgebra homológica, de forma que se pueda ver cómo toda la teoría desarrollada durante las secciones anteriores se puede aplicar a problemas muy distintos, justificando así su estudio.

La primera aplicación presentada es la que se refiere al problema de la extensión de grupos. Como en otras estructuras algebraicas, en el caso de los grupos es interesante en ciertos momentos tener una forma de extenderlos a grupos más grandes. Hablando sin rigor (más adelante se formalizará), para los grupos se habla de extender un grupo G por otro A obteniendo un E a partir del primero que en cierto sentido "contenga" también al segundo. El problema de la extensión de grupos, a grandes rasgos, intenta averiguar de cuántas formas distintas se puede hacer esto, es decir, calcular cuántas extensiones de un grupo por otro existen.

Esta pregunta no es para nada trivial, y aunque sigue sin estar resuelta de forma general el interés en ella es máximo. Esto se debe en parte al caso de los grupos finitos, donde las extensiones cobran una gran importancia. No es difícil de probar que cualquier grupo finito G posee una *serie de composición*, es decir, una familia $\{G_i\}$ de subgrupos de G de forma que

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1,$$

donde cada G_{i+1} es un subgrupo normal, maximal y propio de G_i. Además, en este caso, se puede probar también que cada grupo cociente G_{i+1}/G_i es un grupo simple y no trivial y por el conocido como *Teorema de Jordan-Hölder*, se prueba que cada grupo G determina unívocamente este conjunto de grupos cociente simples.

De esta forma, podemos ver los grupos simples finitos como las piezas que, mediante extensiones, construyen cualquier grupo finito. Recordemos además que uno de los grandes logros matemáticos de las últimas décadas fue obtener una clasificación de los grupos finitos simples. Esto significa que resolver el problema de la extensión de grupos nos acercaría a poder clasificar todos los grupos finitos, lo cual sería un grandísimo hito en la historia del álgebra.

Tras hablar del problema de la extensión de grupos, pasaremos a hablar sobre las aplicaciones que la homología tiene en particular en el campo de la topología algebraica. En la actualidad, este es probablemente el campo de las matemáticas donde el uso del álgebra homológica es más común. Algo lógico por otra parte, ya que como hemos comentado en la introducción, la homología surgió precisamente a partir de ciertos problemas topológicos.

Debido a que sería necesario incluir un gran número de conceptos topológicos que se escapan al alcance del trabajo para poder hablar con rigor de la homología en espacios topológicos, esta segunda aplicación solo se tratará de una forma muy somera, sin entrar en demasiada profundidad. De todas formas sí que se desarrollarán las bases de la homología en espacios topológicos y se explicará en qué situaciones concretas pueden aplicarse herramientas homológicas, además de cómo se pueden construir dichas herramientas en el caso particular de los espacios topológicos.

5.1. Extensiones de grupos

Para llegar al punto central de este apartado, las *extensiones de grupos*, necesitamos en primer lugar introducir los *grupos de cohomología* de un cierto grupo. La definición de estos grupos se puede hacer tanto de forma funtorial como de forma concreta y constructiva. Si bien la primera es más natural, también es mucho más laboriosa, y por esta razón no se recoge aquí. La construcción de estos grupos se hará por tanto de la segunda manera indicada, que también fue la forma clásica en la que surgió y finalmente se dará una equivalencia entre ambas construcciones.

Antes de comenzar, necesitamos definir unas nociones previas:

Definición 5.1 (Módulo sobre un grupo)**.** *Si G es un grupo, podemos definir un G-módulo A como un grupo abeliano (escrito aditivamente) sobre el cual G actúa mediante una aplicación de $G \times A$ en A, $(g, x) \mapsto gx$, tal que*

$$g(x + y) = gx + gy, \quad (g_1g_2)x = g_1(g_2x), \quad 1x = x$$

para todo $g, g_1, g_2 \in G$, $x, y \in A$ (donde 1 representa la identidad en G).

Además, si introducimos el anillo de grupo $\mathbb{Z}[G]$, es decir, el $\mathbb{Z}$-módulo libre con base G donde se tiene además una estructura de anillo definiendo la multiplicación como

$$(\Sigma\alpha_g g)\,(\Sigma\beta_h h) = \Sigma\alpha_g\beta_h gh$$

para todo $\alpha_g, \beta_h \in \mathbb{Z}$, $g, h \in G$; podemos ver inmediatamente que cualquier G-módulo A se convierte en un $\mathbb{Z}[G]$-módulo si definimos la acción

$$(\Sigma\alpha_g g)x = \Sigma\alpha_g(gx)$$

para todo $\Sigma\alpha_g g \in \mathbb{Z}[G]$, $x \in A$. Y además, de forma inversa, si A es un $\mathbb{Z}[G]$-módulo, entonces A se puede convertir en un G-módulo definiendo la acción $gx = (1g)x$ (con la misma notación que en el caso anterior).

Es obvio que se pueden obtener distintos G-módulos según la acción gx elegida. Por ejemplo, para cualquier grupo abeliano A, la acción trivial $gx = x$ para todo $g \in G$, $x \in A$ proporciona a A una estructura de G-módulo que llamaremos trivial.

Sea entonces A un G-módulo, con G un grupo cualquiera. Para un $n = 0, 1, 2, \ldots$, denotaremos como $C^n(G, A)$ al conjunto de funciones de n variables de G en el módulo A. Es decir, que si $n > 0$, entonces $C^n(G, A)$ es el conjunto de aplicaciones de $\underbrace{G \times G \times \cdots \times G}_{n}$ en A, el cual tiene una estructura de grupo abeliano si definimos

$$(f + f')(g_1, \ldots g_n) = f(g_1, \ldots g_n) + f'(g_1, \ldots g_n)$$

para todo $f, f' \in C^n(G, A)$ y $0(g_1, \ldots, g_n) = 0$. Si $n = 0$, cada aplicación anterior se corresponderá con un elemento de A, y entonces $C^0(G, A)$ también tendrá una estructura de grupo abeliano dada por el propio grupo A.

Definimos ahora una aplicación $\delta (= \delta_n)$ de $C^n(G, A)$ a $C^{n+1}(G, A)$ tal que para un $f \in C^n(G, A)$ cualquiera,

$$\begin{aligned} \delta f(g_1, \ldots, g_{n+1}) = {} & g_1 f(g_2, \ldots, g_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, \ldots, g_{n+1}) \\ & + (-1)^{n+1} f(g_1, \ldots, g_n). \end{aligned} \tag{6}$$

De esta forma, si $n = 0$ (en este caso f es simplemente un elemento de A),

$$\delta f(g_1) = g_1 f - f;$$

si $n = 1$,

$$\delta f(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1);$$

si $n = 2$,

$$\delta f(g_1, g_2, g_3) = g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2),$$

y así consecutivamente. Es directo ver que δ es un homomorfismo de grupos entre $C^n(G, A)$ y $C^{n+1}(G, A)$, lo que nos permite asegurar que su núcleo, al que denotaremos como $Z^n(G, A)$, es un subgrupo de $C^n(G, A)$ y su imagen, $B^{n+1}(G, A)$, es también un subgrupo, ahora de $C^{n+1}(G, A)$.

Como además se tiene que $\delta\delta f = 0$ para todo $f \in C^n(G, A)$ y para cada n (algo que no se probará aquí ya que para esta construcción resulta muy engorroso y no aporta nada), entonces podemos concluir que $B^n(G, A) \subseteq Z^n(G, A)$ para todo n. De esta forma, se puede definir el grupo cociente $H^n(G, A) = Z^n(G, A)/B^n(G, A)$, al que llamaremos *$n$-ésimo grupo de cohomología de G con coeficientes en A.*

La construcción anterior, como ya se avisó al principio de este apartado, es bastante artificial. Sin embargo, esta fue la forma en la que surgió el interés por los grupos de cohomología (en concreto para $n = 1$ y $n = 2$), estudiando ciertas cuestiones en teoría de grupos. Mediante la construcción funtorial de los grupos de cohomología se puede llegar a la siguiente, y muy importante, equivalencia:

Teorema 5.2. *Para todo $n = 0, 1, 2, \ldots$, $H^n(G, A) \cong \mathrm{Ext}^n(\mathbb{Z}, A)$, considerando $\mathbb{Z}$ como un G-módulo trivial.*

Las ventajas que esta segunda construcción aporta son muy importantes, ya que todos los resultados funtoriales sobre los funtores Ext pueden ser ahora aplicados a los grupos de cohomología. Por ejemplo, y dando así un ejemplo concreto de un grupo de cohomología:

Proposición 5.3. *$H^0(G, A) \cong A^G$, el subgrupo de A conteniendo aquellos elementos x tales que $gx = x$ para todo $g \in G$.*

Demostración. Como vimos en la sección anterior, $\mathrm{Ext}^0(M, N) \cong \hom(M, N)$. De esta forma, $H^0(G, A) \cong \hom_{\mathbb{Z}[G]}(\mathbb{Z}, A)$, el grupo de los $\mathbb{Z}[G]$-homomorfismos de $\mathbb{Z}$ en A. Si $\eta \in \hom_{\mathbb{Z}[G]}(\mathbb{Z}, A)$, entonces la imagen $\eta(1) = x \in A$ determina η. Pero entonces, esta imagen cumple que $x = \eta(1) = \eta(g1) = g\eta(1) = gx$ para todo $g \in G$. De forma inversa, si $x \in A$ satisface que $gx = x$ para todo $g \in G$, entonces la aplicación η tal que $\eta(n) = nx$ es un $\mathbb{Z}[G]$-homomorfismo de $\mathbb{Z}$ en A. Esto implica que la aplicación $\eta \mapsto \eta(1)$ es un isomorfismo entre los grupos $\hom_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ y A^G. □

Dar unas expresiones algo más manejables de los elementos de los grupos H^1 y H^2 no es tampoco complicado, ya que ambos se pueden construir como unos grupos de homomorfismos con cierta forma específica. Sin embargo, no nos detendremos en esto y pasaremos a dar un resultado para grupos finitos:

Proposición 5.4. *Si G es un grupo finito y A un G-módulo, entonces todo elemento de $H^n(G, A)$, $n > 0$, tiene orden finito y este orden divide a $|G|$.*

Demostración. Sea $f \in C^n(G, A)$ y consideremos la fórmula (6) para δf. En esta fórmula dejaremos el último parámetro, g_{n+1}, libre sobre G y sumaremos todas las posibilidades. De esta forma, obtendremos la suma $\Sigma_{g\in G}(g_1, ..., g_n, g)$ que abreviaremos como $S(g_1, ..., g_n)$. Además, como $\Sigma_{g\in G}(g_1, ..., g_n g) = S(g_1, ..., g_{n-1})$, tenemos que

$$\begin{aligned}\sum_{g\in G} \delta f(g_1, ..., g_n, g) &= g_1 S(g_2, ..., g_n) + \sum_{i=1}^{n-1} (-1)^i S(g_1, ..., g_i g_{i+1}, ..., g_n) + \\ &\quad + (-1)^n S(g_1, ..., g_{n-1}) + (-1)^{n+1} |G| f(g_1, ..., g_n) = \\ &= \delta S(g_1, ..., g_n) + (-1)^{n+1} |G| f(g_1, ..., g_n)\end{aligned}$$

De esta forma, como $\delta f = 0$, entonces $|G| f(g_1, ..., g_n) = \pm \delta S(g_1, ..., g_n) \in B^n(G, A)$. Esto significa que $|G| Z^n(G, A) \subseteq B^n(G, A)$, lo cual implica que $|G| H^n(G, A) = 0$, probando así el resultado. □

Además, como consecuencia de esta proposición se tiene lo siguiente:

Corolario 5.5. *Sea G un grupo finito y A un G-módulo finito tal que $|G|$ y $|A|$ son primos entre sí. Entonces $H^n(G, A) = 1$, el grupo trivial, para todo $n > 0$.*

Demostración. Inmediato por la proposición anterior y que $|A| f = 0$ para todo $f \in C^n(G, A)$. □

Después de esta larga introducción, ya estamos en condiciones de hablar de las extensiones de grupos. De forma similar a lo comentado para módulos en el apartado 4.6, denominamos *extensión del grupo G por un grupo A* a la sucesión exacta corta de grupos $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$, es decir, una sucesión donde i es inyectiva, p es sobreyectiva y $\ker p = \text{im } i$ (además, tendremos que $\text{im } i = iA \lhd E$). Por abreviar, nos referiremos a lo anterior como "la extensión E". Notar que en una extensión como la anterior, $A \lhd E$ (en el sentido de que A será isomorfo a algún subgrupo normal de E) y $E/A \cong G$. De esta forma, la definición de extensión que acabamos de dar es consistente con el objetivo que nos hemos marcado en la introducción a la sección hablando de forma poco rigurosa sobre las series de composición.

Por otro lado, si $1 \to A \xrightarrow{i'} E' \xrightarrow{p'} G \to 1$ es una segunda extensión de G por A, esta se dirá *equivalente* a la anterior si existe un homomorfismo $h : E \to E'$ tal que el diagrama

$$\begin{tikzcd} & E \arrow[dr, "p"] \arrow[dd, "h"] & \\ A \arrow[ur, "i"] \arrow[dr, "i'"'] & & G \\ & E' \arrow[ur, "p'"'] & \end{tikzcd}$$

es conmutativo. En este caso, como para módulos, se sigue inmediatamente que el anterior h debe ser un isomorfismo y las extensiones de G por A se podrán agrupar en clases de equivalencia.

En este apartado nos restringiremos al estudio de las extensiones de un grupo cualquiera G por otro abeliano A. Como ahora veremos, este tipo de extensiones tiene la particularidad de que a cada una se le puede asociar una acción de G sobre A y un elemento del grupo de cohomología $H^2(G, A)$ (viendo A como un G-módulo bajo la acción anterior). Supongamos entonces que tenemos una cierta extensión E de un grupo G por otro grupo abeliano A y veamos que esto se cumple.

Comencemos definiendo la acción de G en A. Sea $\sigma \in G$, $x \in A$. Tomamos entonces un $s \in E$ tal que $ps = \sigma$, y construimos el elemento $s(ix)s^{-1} \in E$. Como iA es un subgrupo normal de E, entonces $s(ix)s^{-1} \in iA$ y como i es inyectiva, tenemos un único elemento $y \in A$ de forma que $s(ix)s^{-1} = iy$. Veamos que este y es independiente del s elegido al principio como preimagen de σ, para ello, sea s' otro elemento de E tal que $ps' = \sigma$. Entonces $p(s's^{-1}) = \sigma\sigma^{-1} = 1$ y por tanto $s's^{-1} = ia$ para un $a \in A$ y $s' = (ia)s$. Como iA es obviamente abeliano, tenemos que $s'(ix)s'^{-1} = (ia)s(ix)s^{-1}(ia)^{-1} = s(ix)s^{-1}$. De esta forma, el anterior y es independiente del s elegido como primer paso para construirlo y queda determinado por σ. Esto significa que podemos definir la acción de G en A como

$$\sigma x = y \quad \text{donde } ps = \sigma,\ s(ix)s^{-1} = iy$$

para todo $\sigma \in G$, $x \in A$.

Verificar que para la aplicación que acabamos de definir se cumple que $(\sigma_1\sigma_2)x = \sigma_1(\sigma_2 x)$, $1x = x$ y $\sigma(xy) = (\sigma x)(\sigma y)$ es directo, lo cual prueba que efectivamente es una acción de G en A y que hemos definido una estructura de G-módulo en A (con la particularidad de que A está ahora escrito de forma multiplicativa, no aditiva, ya que nos interesa más en este desarrollo).

A continuación, veamos cuál es el elemento del segundo grupo de cohomología $H^2(G, A)$ asociado a la extensión E. Para encontrarlo, comenzaremos tomando para cada $\sigma \in G$ un $s_\sigma \in E$ de forma que $ps_\sigma = \sigma$. De esta forma tendremos una aplicación $s : G \to E$, $\sigma \mapsto s_\sigma$ tal que $ps_\sigma = \sigma$ para todo $\sigma \in G$ o dicho de otra forma, $ps = 1_G$.

Sean ahora $\sigma, \tau \in G$ y consideremos el elemento $s_\sigma s_\tau s_{\sigma\tau}^{-1}$ de E. Es obvio que la imagen por p de este elemento es 1, lo que significa que existe un $k_{\sigma,\tau} \in A$ tal que $s_\sigma s_\tau s_{\sigma\tau}^{-1} = ik_{\sigma,\tau}$, o $s_\sigma s_\tau = (ik_{\sigma,\tau})s_{\sigma\tau}$. Si además $\rho \in G$, entonces

$$
\begin{aligned}
s_\rho(s_\sigma s_\tau) = s_\rho(ik_{\sigma,\tau})s_{\sigma\tau} = s_\rho(ik_{\rho,\tau})s_\rho^{-1}s_\rho s_{\sigma\tau} = \\
= i(\rho k_{\sigma,\tau})s_\rho s_{\sigma\tau} = i(\rho k_{\sigma,\tau})i(k_{\rho,\sigma\tau})s_{\rho\sigma\tau} = i((\rho k_{\sigma,\tau})k_{\rho,\sigma\tau})s_{\rho\sigma\tau}.
\end{aligned}
$$

De forma similar, $s_\rho(s_\sigma s_\tau) = i(k_{\rho,\sigma}k_{\rho\sigma,\tau})s_{\rho\sigma\tau}$. Debido a la asociatividad en E y a que i es inyectiva, tenemos entonces que

$$
k_{\rho,\sigma}k_{\rho\sigma,\tau} = (\rho k_{\sigma,\tau})k_{\rho,\sigma\tau}. \tag{7}
$$

Las igualdades obtenidas implican que la aplicación $k : G\times G \to A$ tal que $(\sigma, \tau) \mapsto k_{\sigma,\tau}$ es un elemento de $Z^2(G, A)$ definido de la manera clásica explicada al principio de este apartado (dicho de otra forma, es fácil probar a partir de esto que $\delta k = 0$ con δ según se ha definido antes). Esto signfica además que a la extensión se le puede asociar el elemento de $H^2(G, A)$ determinado por $k \in Z^2(G, A)$.

Veamos ahora que el anterior k no depende de la primera aplicación $s : G \to E$ elegida para su construcción. Sea s' otra aplicación de G a E de forma que $ps' = 1_G$. Entonces, para cada $\sigma \in G$, $p(s'_\sigma s_\sigma^{-1}) = (ps'_\sigma)(ps_\sigma)^{-1} = \sigma\sigma^{-1} = 1$ y nuevamente existirá un único $u_\sigma \in A$ de forma que $s'_\sigma s_\sigma^{-1} = iu_\sigma$ o $s'_\sigma = (iu_\sigma)s_\sigma$. Hemos construido así una aplicación u de G en A, $u(\sigma) = u_\sigma$ de forma que para todo $\sigma \in G$, $s'_\sigma = (iu_\sigma)s_\sigma$.

Pero si u es una aplicación cualquiera de G en A, entonces una aplicación s' definida por la última igualdad dada, $s'(\sigma) = s'_\sigma = (iu_\sigma)s_\sigma$, cumple que $ps' = 1_G$. Además, por todas las igualdades anteriores tenemos que

$$
\begin{aligned}
s'_\sigma s'_\tau = (iu_\sigma)s_\sigma(iu_\tau)s_\tau = i(u_\sigma(\sigma u_\tau))s_\sigma s_\tau = \\
= i(u_\sigma(\sigma u_\tau)k_{\sigma,\tau})s_{\sigma\tau} = i(u_\sigma(\sigma u_\tau)k_{\sigma,\tau}u_{\sigma\tau}^{-1})s'_{\sigma\tau}.
\end{aligned}
$$

De esta forma, el cambio de s a s' implica un cambio de la aplicación k a otra k' de forma que

$$
k'_{\sigma,\tau} = u_\sigma(\sigma u_\tau)u_{\sigma\tau}^{-1}k_{\sigma,\tau}.
$$

Obviamente, $k' : G \times G \to A$ es un elemento de $Z^2(G, A)$ y a partir de la relación anterior es directo ver que determina el mismo elemento del cociente $H^2(G, A)$ que k. De esta forma, es la propia extensión E la que determina unívocamente un elemento en $H^2(G, A)$.

Hemos visto hasta aquí cómo una extensión de un grupo cualquiera G por otro abeliano A determina una acción de A en G y un elemento del segundo grupo de cohomología $H^2(G, A)$. Pero es más, se puede probar que estos dos elementos determinados por una extensión no varían dentro de una misma clase de equivalencia de extensiones, como se verá a continuación.

Teorema 5.6. *Dos extensiones de un grupo G por otro abeliano A son equivalentes si y solamente si determinan la misma acción de G en A y el mismo elemento de $H^2(G, A)$.*

Demostración. Sean $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ y $1 \to A \xrightarrow{i'} E' \xrightarrow{p'} G \to 1$ dos extensiones de G por A. La implicación directa es obvia por la construcción que acabamos de hacer, teniendo en cuenta el isomorfismo existente entre E y E'. Probaremos en detalle la inversa. Para ello, veremos que la multiplicación en E queda determinada por la acción de G en A y la aplicación $k : G \times G \to A$ de la construcción anterior. Sea $e \in E$ y $\sigma = pe \in G$, $f = e(s_\sigma)^{-1}$ (nótese que se sigue la notación de la construcción anterior). Entonces, $pf = pe(ps_\sigma)^{-1} = \sigma\sigma^{-1} = 1$, con lo que $f = ix$ para algún $x \in A$ unívocamente determinado. De esta forma, tendremos la factorización

$$e = (ix)s_\sigma, \quad x \in A, \ \sigma \in G,$$

donde tanto x como σ quedan unívocamente determinados por el elemento $e \in E$ escogido. Consideremos ahora $e' = (iy)s_\tau$ un segundo elemento de E. Entonces, el producto ee' en E es igual a

$$(ix)s_\sigma(iy)s_\tau = i(x(\sigma y))s_\sigma s_\tau = i(x(\sigma y)k_{\sigma,\tau})s_{\sigma\tau}. \tag{8}$$

Supongamos ahora la hipótesis, es decir, que las extensiones E y E' determinan la misma acción de G en A (y por tanto la misma estructura de módulo en A) y el mismo elemento de $H^2(G, A)$. Entonces, podemos tomar dos aplicaciones s y s' de G en E y E' respectivamente de forma que $ps = 1_G$, $p's' = 1_G$ y que para cualesquiera dos elementos $\sigma, \tau \in G$, tengamos que $s_\sigma s_\tau = (ik_{\sigma,\tau})s_{\sigma\tau}$ y $s'_\sigma s'_\tau = (i'k_{\sigma,\tau})s'_{\sigma\tau}$. De esto se tiene directamente (8) para la extensión E y una igualdad similar para E', $(i'x)s'_\sigma(i'y)s'_\tau = i'(x(\sigma y)k_{\sigma,\tau})s'_{\sigma\tau}$. De esto se deduce que la aplicación $h : (ix)s_\sigma \mapsto (i'x)s'_\sigma$ es un homomorfismo de E a E' de forma que el diagrama

$$\begin{tikzcd}
& E \arrow[dd, "h"] \arrow[dr, "p"] & \\
A \arrow[ur, "i"] \arrow[dr, "i'"'] & & G \\
& E' \arrow[ur, "p'"'] &
\end{tikzcd}$$

es conmutativo. Por tanto, las dos extensiones E y E' son equivalentes, finalizando así la demostración. □

Este teorema se completa con el siguiente resultado:

Teorema 5.7. *Sea G un grupo y A un grupo abeliano con una cierta estructura de G-módulo. Se tiene entonces una correspondencia 1-1 entre el conjunto de las clases de equivalencia de las extensiones de G por A con dicha estructura de G-módulo y los elementos del grupo $H^2(G, A)$.*

Demostración. Para probar este resultado, basta ver que dado un G-módulo A y una aplicación $k : G \times G \to A$ satisfaciendo (7), existe una extensión $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ con acción de G en A asociada la dada sobre A y cuyo elemento de $H^2(G, A)$ asociado es el que determina k. Tomamos $E = A \times G$, el conjunto de pares (x, σ) con $x \in A$, $\sigma \in G$ y definimos una multiplicación en E como

$$(x, \sigma)(y, \tau) = (x(\sigma y)k_{\sigma,\tau}, \sigma\tau).$$

Es inmediato por (7) que esta multiplicación es asociativa. Además, si tomamos en esta igualdad $\rho = \sigma = 1$, se obtiene que $k_{1,1}k_{1,\tau} = k_{1,\tau}k_{1,\tau}$, de donde $k_{1,\tau} = k_{1,1}$ y entonces

$$(k_{1,1}^{-1}, 1)(y, \tau) = (k_{1,1}^{-1}yk_{1,\tau}, \tau) = (y, \tau)$$

por lo que $(k_{1,1}^{-1}, 1)$ es una unidad a izquierda en E. Además, también lo es a derecha ya que todo elemento $(x, \sigma) \in E$ tiene un inverso a izquierda relativo a esta unidad:

$$(k_{1,1}^{-1}k_{\sigma^{-1},\sigma}^{-1}\sigma^{-1}x^{-1}, \sigma^{-1})(x, \sigma) = (k_{1,1}^{-1}k_{\sigma^{-1},\sigma}^{-1}(\sigma^{-1}x^{-1})(\sigma^{-1}x)k_{\sigma^{-1},\sigma}, 1) = (k_{1,1}^{-1}, 1).$$

De esta forma, hemos probado que $E = A \times G$ con la multiplicación arriba definida es en efecto un grupo. Veamos ahora que se puede construir una extensión con este grupo. Para ello, construimos las aplicaciones $i : A \to E$ de forma que $ix = (xk_{1,1}^{-1}, 1)$ para todo $x \in A$ y $p : E \to G$ tal que $p(x, \sigma) = \sigma$ para todo $(x, \sigma) \in E$. Es obvio que i es inyectiva y p sobreyectiva. Además, es inmediato probar que $iA = \ker p$ y que por tanto $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ es una extensión de G por A. Para determinar la acción de G sobre A asociada a esta extensión, notemos que $p(1, \sigma) = \sigma$, por lo que tenemos que calcular

$$(1, \sigma)ix(1, \sigma)^{-1} = (1, \sigma)(xk_{1,1}^{-1}, 1)(1, \sigma)^{-1} = (1, \sigma)(xk_{1,1}^{-1}, 1)(k_{1,1}^{-1}k_{\sigma^{-1},\sigma}^{-1}, \sigma^{-1}).$$

Ahora, de la igualdad (7) podemos obtener varios casos particulares interesantes. En primer lugar, ya hemos visto que $k_{1,\rho} = k_{1,1}$. Además, si tomamos $\sigma = \tau = 1$, obtenemos que $k_{\rho,1}k_{\rho,1} = (\rho k_{1,1})k_{\rho,1}$, de donde $k_{\rho,1} = (\rho k_{1,1})$. Por último, tomando $\sigma = \rho^{-1}$ y $\tau = \rho$ en la misma igualdad, se tiene $k_{\rho,\rho^{-1}}k_{1,\rho} = (\rho k_{\rho^{-1},\rho})k_{\rho,1}$, por lo que $k_{\rho,\rho^{-1}}k_{1,1} = (\rho k_{\rho^{-1},\rho})k_{\rho,1}$. Sustituyendo esto en el cálculo anterior,

$$\begin{aligned}
(1, \sigma)(xk_{1,1}^{-1}, 1)(k_{1,1}^{-1}k_{\sigma^{-1},\sigma}^{-1}, \sigma^{-1}) &= ((\sigma k_{1,1}^{-1})\sigma x k_{\sigma,1}, \sigma)(k_{1,1}^{-1}k_{\sigma^{-1},\sigma}^{-1}, \sigma^{-1}) \\
&= (\sigma x, \sigma)(k_{1,1}^{-1}k_{\sigma^{-1},\sigma}^{-1}, \sigma^{-1}) \\
&= ((\sigma x)\sigma(k_{1,1}^{-1})^{-1}\sigma(k_{\sigma^{-1},\sigma})^{-1}k_{\sigma,\sigma^{-1}}, 1) \\
&= ((\sigma x)k_{\sigma,1}^{-1}\sigma(k_{\sigma^{-1},\sigma})^{-1}k_{\sigma,\sigma^{-1}}, 1) \\
&= ((\sigma x)k_{1,1}^{-1}, 1)
\end{aligned}$$

De esta forma se ha llegado a que $(1, \sigma)ix(1, \sigma)^{-1} = ((\sigma x)k_{1,1}^{-1}, 1)$, lo que implica que la acción de G sobre A es la acción ya dada. Ahora, sea s la aplicación $\sigma \mapsto (1, \sigma)$ de G en E, de forma que $ps = 1_G$. Tenemos que $(1, \sigma)(1, \tau) = (k_{\sigma,\tau}, \sigma\tau) = (k_{1,1}^{-1}k_{\sigma,\tau}, 1)(1, \sigma\tau)$, lo que implica que $s_\sigma s_\tau = (ik_{\sigma,\tau})s_{\sigma\tau}$. De esta forma comprobamos que el elemento de $H^2(G, A)$ asociado a la extensión es el que determina k, lo cual completa la demostración. □

De esta forma hemos asociado (bajo ciertas condiciones) las extensiones de un grupo con los elementos del segundo grupo de cohomología, consiguiendo además con esta identificación facilitar en gran medida la clasificación de extensiones. Esta clasificación de extensiones (aunque clásicamente se planteó de forma ligeramente distinta) es efectivamente la forma en la que surgió el interés por la teoría aquí presentada.

Un caso particular de extensiones son aquellas que *se escinden*. De forma análoga a las sucesiones exactas cortas, una extensión de grupos $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ se dice que se escinde si existe un homomorfismo de grupos $s : G \to E$ de forma que $ps = 1_G$. Según la construcción antes hecha, en este caso se tendrá que $s_\sigma s_\tau = s_\sigma \tau$ para cualesquiera $\sigma, \tau \in G$ y entonces el elemento $k_{\sigma,\tau}$ determinado como antes deberá ser 1. De forma inversa, si el elemento del grupo de cohomología asociado a la extensión es la identidad, entonces tendremos una aplicación $s : G \to E$ de forma que $ps = 1_G$ para la cual todos los $k_{\sigma,\tau}$ son 1. Esto significa que s es un homomorfismo, lo que a su vez implica que la extensión se escinde. De esto podemos concluir que $H^2(G, A) = 1$, el grupo trivial, si y solamente si todas las extensiones de G por A con la estructura de G-módulo en A dada se escinden. Nótese que por el corolario 5.5, este será el caso si G y A son finitos con $|G|$ y $|A|$ primos entre sí.

Ahora, si $E/A = G$ para un cierto $A \lhd E$ no necesariamente abeliano, podremos construir la extensión $1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$ donde i es la inclusión de A en E y p es el homomorfismo canónico de E en un cociente suyo. Es directo ver que esta extensión se escinde si y solamente si existe un subgrupo S de E de forma que $E \cong S \times A$ y $S \cap A = 1$. En este caso E se dice además *producto semidirecto de S y A*. Sobre este tipo de extensiones se tiene el siguiente teorema, el cual no se probará por no alargar más esta sección pero tiene bastante interés:

Teorema 5.8. *Sea E un grupo finito y A un subgrupo normal de E de forma que $|A|$ y $|E/A|$ sean primos entre sí. Entonces E es un producto semidirecto de A y un subgrupo S de E.*

Finalizaremos esta sección con un par de ejemplos. Para el primero, calcularemos las extensiones de $\mathbb{Z}_2$ por el grupo $\mathbb{Z}_3$. En primer lugar, notemos que una acción de un grupo sobre otro definida como en la definición 5.1 puede verse como un homomorfismo entre el primero de los grupos y el grupo de automorfismos del segundo. De esta forma, para enumerar todas las acciones posibles en nuestro caso necesitaremos calcular el grupo $\hom(\mathbb{Z}_2, \mathrm{Aut}(\mathbb{Z}_3))$. El grupo de automorfismos de $\mathbb{Z}_3$ contiene solamente la aplicación identidad y la inversa (en donde la imagen de $\bar{1}$ es $\bar{2}$ y viceversa). Esto implica que solamente hay dos acciones posibles de $\mathbb{Z}_2$ sobre $\mathbb{Z}_3$. Vistas como homomorfismos, las dos acciones son: una primera trivial ρ_0 de forma que tanto $\rho_0(\bar{0})$ como $\rho_0(\bar{1})$ son la aplicación identidad en $\mathbb{Z}_3$ y otra ρ_1 tal que $\rho_1(\bar{0})$ es la aplicación identidad y $\rho_1(\bar{1})$ es la aplicación inversa.

De esta forma, podremos extender $\mathbb{Z}_2$ por $\mathbb{Z}_3$ de, al menos, dos formas no isomorfas, dando a $\mathbb{Z}_3$ estructura de $\mathbb{Z}_2$-módulo a partir de cada una de las dos acciones antes definidas. Por el corolario 5.5, como 2 y 3 son primos entre sí, tenemos que los grupos $H^2(\mathbb{Z}_2, \mathbb{Z}_3)$ obtenidos al considerar las dos acciones distintas de $\mathbb{Z}_2$ sobre $\mathbb{Z}_3$ son ambos triviales, de forma que por el teorema 5.7, tenemos que hay exactamente dos clases de equivalencia de extensiones de $\mathbb{Z}_2$ por $\mathbb{Z}_3$.

Los cálculos para averiguar a qué grupo corresponde cada una de estas dos extensiones son algo extensos, por lo que se omitirán aquí. Se tiene que la acción trivial (la anterior ρ_0) lleva a la construcción del grupo $\mathbb{Z}_6$. Es inmediato que esta extensión es además un producto semidirecto, pero al estar construida a partir de la acción trivial no se le dice así sino que se le denomina *producto directo* (lo cual es consistente con la definición de producto directo típicamente vista en teoría de grupos, con la cual también se tiene que $\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$). Por otro lado, la acción no trivial (es decir, ρ_1) lleva a la construcción del grupo simétrico S_3. Esta extensión, que también es un producto semidirecto, sí que recibe normalmente este nombre. Además, es inmediato comprobar que efectivamente, las dos extensiones obtenidas no son isomorfas ($\mathbb{Z}_6$ es abeliano y S_3 no) y que existen homomorfismos i, p, i', p' tales que las sucesiones

$$1 \longrightarrow \mathbb{Z}_3 \xrightarrow{i} \mathbb{Z}_6 \xrightarrow{p} \mathbb{Z}_2 \longrightarrow 1,$$
$$1 \longrightarrow \mathbb{Z}_3 \xrightarrow{i'} S_3 \xrightarrow{p'} \mathbb{Z}_2 \longrightarrow 1.$$

son exactas (formando así dos extensiones según se han definido antes). Estos homomorfismos son la inclusión y proyección canónica sobre un producto en el primer caso (recordemos que $\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$). En el segundo caso, i' es el homomorfismo tal que $i'(\bar{0}) = \mathrm{Id}$, $i'(\bar{1}) = (123)$ y $i'(\bar{2}) = (132)$ y p' es el homomorfismo que manda los tres elementos en la imagen de i' a $\bar{0}$ y los tres elementos de S_3 restantes a $\bar{1}$.

Consideremos ahora un segundo ejemplo donde el grupo de homología no es el trivial: las extensiones del grupo $\mathbb{Z}_2$ por sí mismo. Comencemos viendo que la única acción de $\mathbb{Z}_2$ sobre él mismo es la trivial. Esto se debe a que en este caso el grupo de automorfismos $\mathrm{Aut}(\mathbb{Z}_2)$ tan solo contiene la aplicación identidad, lo cual implica que solo existe un elemento en $\hom(\mathbb{Z}_2, \mathrm{Aut}(\mathbb{Z}_2))$, la acción que lleva ambos elementos de $\mathbb{Z}_2$ al automorfismo identidad.

Antes de entrar a calcular el grupo de cohomología, sabemos además que tanto el grupo cíclico $\mathbb{Z}_4$ como el grupo de Klein $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ tienen un subgrupo normal isomorfo a $\mathbb{Z}_2$ y cumplen que $\mathbb{Z}_4/\mathbb{Z}_2 \cong \mathbb{Z}_2 \cong V_4/\mathbb{Z}_2$. Esto significa que ambos grupos son extensiones de $\mathbb{Z}_2$ por él mismo. Además, las dos extensiones no son equivalentes, ya que V_4 no tiene elementos de orden 4 y $\bar{1} \in \mathbb{Z}_4$ tiene orden 4, lo que significa que estos grupos no son isomorfos. Esto prueba que al menos existen dos clases de equivalencia de extensiones de $\mathbb{Z}_2$ por sí mismo (tomando para construirlas la única acción posible).

Para concluir el ejemplo, veamos que $H^2(\mathbb{Z}_2, \mathbb{Z}_2) \cong \mathbb{Z}_2$, por lo que las dos extensiones antes mencionadas serán las únicas existentes. Recordamos para ello que $H^2(\mathbb{Z}_2, \mathbb{Z}_2)$ se construía como el cociente $Z^2(\mathbb{Z}_2, \mathbb{Z}_2)/B^2(\mathbb{Z}_2, \mathbb{Z}_2)$, donde $Z^2(\mathbb{Z}_2, \mathbb{Z}_2) = \delta C^1(\mathbb{Z}_2, \mathbb{Z}_2)$, con la aplicación δ definida como (6) y $C^1(\mathbb{Z}_2, \mathbb{Z}_2)$ es el conjunto de aplicaciones de $\mathbb{Z}_2$ en $\mathbb{Z}_2$. Es obvio que $C^1(\mathbb{Z}_2, \mathbb{Z}_2)$ tiene orden 4. En concreto, se tiene que $C^1(\mathbb{Z}_2, \mathbb{Z}_2) = \{f_{0,0}, f_{0,1}, f_{1,0}, f_{1,1}\}$ (denotando cada elemento con dos subíndices según las imágenes de $\bar{0}$ y $\bar{1}$ y omitiendo las barras por claridad). Componiendo estas cuatro aplicaciones con δ, se tiene por un lado que $\delta f_{0,0} = \delta f_{0,1}$ y ambas son iguales a la aplicación nula. Por otro lado, $\delta f_{1,0} = \delta f_{1,1}$, ambas aplicaciones mandando los elementos $(\bar{0}, \bar{0})$ y $(\bar{0}, \bar{1})$ al $\bar{0}$, así como $(\bar{1}, \bar{0})$ y $(\bar{1}, \bar{1})$ al $\bar{1}$. De esta forma, $Z^2(\mathbb{Z}_2, \mathbb{Z}_2)$ tiene orden 2, lo que implica que $H^2(\mathbb{Z}_2, \mathbb{Z}_2)$ tiene orden a lo sumo 2. Pero por otro lado, la existencia de dos extensiones no equivalentes para la única acción posible implica que el orden de $H^2(\mathbb{Z}_2, \mathbb{Z}_2)$ es al menos 2. De esta forma, $H^2(\mathbb{Z}_2, \mathbb{Z}_2) \cong \mathbb{Z}_2$ y las extensiones antes indicadas forman las dos únicas clases de equivalencia de las extensiones de $\mathbb{Z}_2$ por él mismo.

5.2. Aplicaciones a la topología algebraica

Como broche final al trabajo, se recoge en este apartado una pequeñísima introducción a cómo puede la topología algebraica aprovecharse de las herramientas homológicas. Si bien esto se desvía un poco del carácter puramente algebraico del trabajo, introducir estas aplicaciones de la homología a la topología hace justicia a la forma en la que históricamente surgió la teoría que aquí desarrollamos. Además de esto, nos permitirá ver cómo realmente la teoría de homología que ha sido desarrollada durante el trabajo trasciende lo puramente algebraico.

Recordaremos para comenzar que un *espacio topológico* es un par (X, τ) donde X es un conjunto y τ una *topología* sobre X, es decir, una familia de subconjuntos de X cerrada por uniones arbitrarias e intersecciones finitas de forma que $\emptyset, X \in \tau$. A los elementos de τ se les dice *conjuntos abiertos* y para abreviar, si no hay lugar a dudas, denotaremos el espacio topológico simplemente como X.

Necesitaremos además el concepto de *n-símplice*. En un espacio $\mathbb{R}^m$ un n-símplice es el menor *conjunto convexo*[1] que contiene a $n+1$ puntos $v_0, ..., v_n$ de forma que los vectores $v_1 - v_0, ..., v_n - v_0$ sean linealmente independientes. Denotaremos este n-símplice como $[v_0, ..., v_n]$. Si definimos para cada $n \geq 0$ el conjunto Δ^n como

$$\Delta^n = \{(t_0, ..., t_{n-1}) \in \mathbb{R}^{n+1} : \sum_{i=0}^{n} t_i = 1,\ t_i \geq 0 \text{ para todo } i\},$$

(podemos comprobar que Δ^0 es un punto, Δ^1 un segmento, Δ^2 un triángulo y así sucesivamente), cualquier n-símplice $[v_0, ..., v_n]$ podrá identificarse con una aplicación continua[2] $\sigma : \Delta^n \to \mathbb{R}^m$, $\sigma(t_0, ..., t_n) = \sum t_i v_i$ de forma que im $\sigma = [v_0, ..., v_n]$. Esta identificación permite generalizar el concepto de n-símplice a espacios topológicos X cualesquiera, en donde llamaremos *n-símplice (singular)* a una aplicación continua $\sigma : \Delta^n \to X$.

Como ya dijimos al principio de la sección 4, los complejos forman la noción básica del álgebra homológica. Es por eso que tiene sentido comenzar definiendo qué es un complejo en el contexto de la topología.

Para llegar a esto, comenzamos considerando $C_n(X)$ como el grupo abeliano libre (es decir, $\mathbb{Z}$-módulo libre) generado por los n-símplices en un espacio topológico cualquiera X. A este grupo le diremos *grupo de n-cadenas (singulares)* y sus elementos serán de la forma $\Sigma_i k_i \sigma_i$ con $k_i \in \mathbb{Z}$ (entendiendo esta notación como una suma formal

[1]Recordamos que un *conjunto convexo* es aquél en el que los segmentos entre dos puntos cualesquiera están contenidos en el propio conjunto. Además, notamos que siempre que no se indique qué topología está siendo usada en un espacio real, supondremos que trabajamos con la topología euclídea.

[2]En un contexto topológico, recordemos que una aplicación se dice *continua* si la preimagen de cualquier abierto en el espacio destino es abierta en el espacio de origen.

entre aplicaciones).

Además, definimos el *operador borde* $\delta_n : C_n(X) \to C_{n-1}(X)$ como

$$\delta_n(\sigma) = \sum_i (-1)^i \sigma|_{[v_0,\dots,v_n]\setminus[v_i]}$$

para todo n-símplice σ, donde la restricción $\sigma|_{[v_0,\dots,v_n]\setminus[v_i]}$ denota el n-símplice obtenido a partir de σ eliminando el i-ésimo vértice. Este operador puede extenderse por linealidad a un homomorfismo de grupos entre $C_n(X)$ y $C_{n-1}(X)$ de forma que

$$\delta_n\left(\sum_i k_i\sigma_i\right) = \sum_i k_i\delta_n(\sigma_i)$$

para cualquier elemento $\Sigma_i k_i\sigma_i \in C_n(X)$.

Habiendo definido una familia de grupos abelianos libres $\{C_n(X)\}$ y una familia de homomorfismos entre ellos $\{\delta_n : C_n(X) \to C_{n-1}(X)\}$, podemos construir la siguiente sucesión:

$$\cdots \to C_{n+1}(X) \xrightarrow{\delta_{n+1}} C_n(X) \xrightarrow{\delta_n} C_{n-1}(X) \to \cdots \to C_1(X) \xrightarrow{\delta_1} C_0(X) \xrightarrow{\delta_0} 0. \tag{9}$$

Si probamos que para todo n la composición $\delta_{n-1}\delta_n = 0$, la sucesión anterior formará un complejo de cadenas. Y efectivamente, si $\sigma \in C_n$, entonces

$$\begin{aligned}\delta_{n-1}\delta_n(\sigma) &= \delta_{n-1}\left(\sum_i (-1)^i \sigma|_{[v_0,\dots,v_n]\setminus[v_i]}\right) = \sum_i (-1)^i \delta_{n-1}\left(\sigma|_{[v_0,\dots,v_n]\setminus[v_i]}\right) = \\ &= \sum_{j<i} (-1)^i(-1)^j \sigma|_{[v_0,\dots,v_n]\setminus[v_j,v_i]} + \sum_{j>i} (-1)^i(-1)^{j-1} \sigma|_{[v_0,\dots,v_n]\setminus[v_i,v_j]} = 0.\end{aligned}$$

Esto implica que en el complejo (9) se pueden definir para cada $n \geq 0$ los subgrupos $Z_n(X) = \ker\delta_n$ y $B_n(X) = \operatorname{im}\delta_{n+1}$, los cuales además verificarán en todo caso que $B_n(X) \subseteq Z_n(X)$. De esta forma, podremos definir el n-ésimo grupo de homología para un espacio topológico X como $H_n(X) := Z_n(X)/B_n(X)$, de forma análoga a lo que ya hicimos en el apartado 3.2. Nótese que tras esta construcción particular para los espacios topológicos, se descubre la razón de llamar n-ciclos a los elementos de $Z_n(X)$ y n-bordes a los de $B_n(X)$, algo que ya se introdujo en el mismo apartado 3.2.

Este complejo de cadenas determinado para cada espacio topológico, así como en concreto los grupos de homología, tienen una gran importancia a la hora de determinar ciertas propiedades del espacio topológico. Pero antes de nada, a continuación daremos un resultado que permite tener una idea de cómo son estos grupos de homología.

Proposición 5.9. *Sea $\{X_k\}$ la familia de componentes conexas por caminos*[3] *de un espacio topológico X. Entonces, $H_n(X) \cong \oplus_k H_n(X_k)$.*

[3]Un espacio topológico se dice *conexo por caminos* si para dos puntos cualesquiera a y b del espacio, existe una aplicación continua del intervalo $[0,1]$ en dicho espacio de forma que la imagen de 0 sea igual a a y la imagen de 1 igual a b. No es complicado ver que todo espacio topológico puede descomponerse en la unión disjunta de unos subconjuntos conexos por caminos que se dicen *componentes conexas por caminos*. Además, aunque no se probará aquí, el Δ_n anteriormente definido es conexo por caminos.

Demostración. El isomorfismo buscado surge a partir de otro que, como probaremos a continuación, se tiene entre $C_n(X)$ y $\oplus_k C_n(X_k)$. Como Δ^n es conexo por caminos y σ una aplicación continua, entonces $\sigma\Delta^n$ es también conexo por caminos. De esta forma, para cada n-símplice en X, $\sigma\Delta^n \subseteq X_k$ para alguna componente conexa por caminos X_k de X. Así, cada n-cadena $c \in C_n(X)$ se descompondrá de forma única como $c = \sum_k c_k$, con c_k una n-cadena en X_k, descomposición que nos da el isomorfismo buscado. $\square$

En concreto, y aunque no lo probaremos aquí por no extendernos demasiado, se tiene que si X es no vacío y conexo por caminos, el grupo de homología $H_0(X) \cong \mathbb{Z}$. Esto implica que para cualquier espacio topológico X, $H_0(X)$ es la suma directa de tantas copias de $\mathbb{Z}$ como componentes conexas por caminos formen X.

Debido a que para seguir desarrollando más las aplicaciones a la topología se necesitaría introducir bastante más teoría y esta queda fuera del alcance de este trabajo, a partir de ahora simplemente se comentarán por encima algunas aplicaciones de la homología a la topología algebraica, sin un desarrollo formal. Siguiendo lo que ya hemos hecho para los complejos de cadenas, toda la teoría homológica introducida en la sección 4 puede ser reescrita para el caso particular de los espacios topológicos. Esto nos permitirá desarrollar herramientas que pueden ser directamente aplicables en un contexto topológico.

Por ejemplo, la noción de homotopía (ahora entre aplicaciones continuas) se convierte en que dos aplicaciones continuas $f, g : X \to Y$ se dirán homotópicas si existe otra aplicación continua $H : [0,1] \times X \to Y$ tal que $H(0,x) = f(x)$ y $H(1,x) = g(x)$. Esta definición resulta similar a la que ya teníamos (en este caso particular) y tiene las mismas propiedades: por ejemplo, dos aplicaciones homotópicas siguen induciendo la misma aplicación entre los grupos de homología. Sin embargo, al haberla particularizado, podemos ahora usar la nueva definición para introducir el concepto de *equivalencia homotópica*, una equivalencia más débil que la existente entre espacios homeomorfos[4] pero que en ciertas ocasiones puede ser tan útil como la última o incluso más:

Definición 5.10 (Espacios homotópicamente equivalentes)**.** *Dos espacios topológicos X e Y se dicen homotópicamente equivalentes o que tienen el mismo tipo de homotopía si existen aplicaciones continuas $f : X \to Y$ y $g : Y \to X$ de forma que $gf \sim \mathrm{Id}_X$ y $fg \sim \mathrm{Id}_Y$, las aplicaciones identidad en X e Y respectivamente. Esta relación se suele denotar como $X \simeq Y$ y las aplicaciones f y g se dicen equivalencias homotópicas.*

En algunas ocasiones, esta homología "singular" que hasta aquí hemos introducido se queda corta. Es por eso que paralelamente surgen otras teorías similares que, entre otras cosas, dan formas ligeramente distintas de calcular los grupos de homología de un espacio topológico y que están relacionadas con otros conceptos antes vistos. Estas otras teorías permiten abordar más fácilmente ciertos problemas.

Por ejemplo, la *homología reducida* surge a partir de los complejos de cadenas aumentados y consigue que los grupos de homología de cualquier punto sean triviales. Por otro lado, la *homología relativa* relaciona la homología de un espacio X con la de

[4]Dos espacios topológicos X e Y se dicen *homeomorfos* si existe un *homeomorfismo* entre ellos, es decir, una aplicación continua, biyectiva y con inversa continua.

un subespacio $A \subseteq X$ y se construye usando las sucesiones exactas cortas de complejos y la sucesión exacta larga de homología que surge a partir de cada una de las primeras. También otras nociones como la de escisión tienen relevancia y así se comienza un largo etcétera de conceptos del álgebra homológica que pueden ser particularizados para los espacios topológicos.

Por último, es obvio que todas estas herramientas homológicas (aplicadas al caso particular de los espacios topológicos) sirven para dar un gran impulso a la teoría existente. En concreto, como ya hemos visto, se pueden dar resultados sobre equivalencia de espacios topológicos, lo cual ayuda a su clasificación y a la identificación de ciertas propiedades en dichos espacios. Pero la homología también sirve para probar resultados tan importantes como el *teorema del punto fijo de Brouwer*[5] o para dar una definición del concepto de *grupo fundamental*, un grupo asociado a cada punto de un espacio topológico que da mucha información sobre cómo es dicho espacio.

[5]Este teorema, usado en un gran número de áreas dentro de las mátematicas, tiene bastantes formulaciones distintas. Una de las más comunes afirma que toda aplicación continua de un disco n-dimensional cerrado en sí mismo tiene al menos un punto fijo (es decir, cuya imagen es él mismo).

6. Conclusiones

En esta memoria, pese a las limitaciones existentes relativas entre otros aspectos a su extensión, podemos considerar que se ha conseguido un buen resumen del trabajo y estudio realizados durante varios meses.

Si bien un gran número de puntos muy relevantes para el álgebra homológica y otras disciplinas han tenido que dejarse de lado, como se ha ido comentando durante el trabajo, la teoría aquí desarrollada creemos que se puede considerar lo suficientemente robusta y relevante como para considerar esta memoria un buen punto de partida a la hora de iniciarse en el estudio de la homología. Esto es reforzado también por el carácter didáctico que en todo momento se le ha intentado dar a lo escrito.

Sin embargo, el trabajo desarrollado a lo largo de esta memoria solamente es una primera aproximación algebraica al mundo de la homología, una teoría mucho más extensa con una cantidad de aplicaciones que van bastante más allá de lo que aquí se ha presentado. De la misma forma, tanto la teoría de módulos como la de categorías que aquí se presentan son meras aproximaciones a estos campos tan amplios. Pero en ningún momento creemos que todas estas carencias en la memoria deban ser vistas precisamente como un punto malo. En todo caso deben ser vistas como puertas a un estudio más a fondo de cada uno de los temas que aquí se tocan, estudio que queda fuera del alcance de un trabajo como este.

Haciendo también una pequeña reflexión sobre el contenido del trabajo, me parece interesante acabar con un comentario más sobre la utilidad de la homología. Teorías de un nivel tan abstracto como el álgebra homológica o las categorías reciben no pocas críticas referidas a la lejanía entre ellas y lo percibido como "mundo real". Sin embargo, con la mera introducción realizada en este trabajo ya hemos visto las aplicaciones tan interesantes que esta teoría tiene. En general, el potencial que la homología tiene al ser desarrollada más en profundidad es inmenso, trascendiendo a las matemáticas puras y siendo usada en otras áreas científicas como la física y la topología computacional, entre otros ejemplos.

Todas estas posibilidades que la homología ofrece la hacen digna de un estudio más en profundidad y justifican completamente el interés del trabajo que se ha presentado en esta memoria.

Referencias

[1] Cartan, H. & Eilenberg, C. (1956). *Homological Algebra.* 1ª ed. Princeton, Nueva Jersey: Princeton University Press.

[2] Dieudonné, J. (2009). *A History of Algebraic and Differential Topology, 1900-1960.* Boston: Birkhäuser.

[3] Grove, L. (1983). *Algebra.* Nueva York: Academic Press, Inc.

[4] Jacobson, N. (1989). *Basic Algebra II.* 2ª ed. New York: W. H. Freeman and Company.

[5] Pulido, M. (2015). *Topología algebraica: Homología singular.* Universidad Complutense de Madrid, Madrid.